GESTIONE CREDENZIALI

Gestione credenziali personali (CNS) e applicative (A2A)

Manuale di gestione delle credenziali per utenti dotati di CNS e certificati X509 per le funzionalità Application To Application (A2A)

Gestione credenziali

Gestione credenziali personali (CNS) e applicative (A2A)

Versione 1.4

Sommario

Contesto

Il presente manuale ha lo scopo di guidare l'utente verso un utilizzo consapevole della procedura di registrazione e gestione delle credenziali personali e applicative. Tali credenziali sono necessarie per autenticarsi verso i sistemi informatici che erogano i servizi applicativi.

Al termine del documento sono riportate le risposte alle domande poste più frequentemente al servizio di supporto (FAQ).

La descrizione dell'utilizzo delle interfacce applicative è fuori dal contesto di questo documento e la si rimanda alla documentazione dello specifico progetto.

Credenziali personali - Carta Nazionale dei Servizi (CNS)

Per accedere alla procedura di gestione delle credenziali applicative è necessario essere in possesso di una CNS[1] in corso di validità. Solo la prima volta è necessario registrare la propria identità registrando i dati della CNS, completando il profilo utente con i dati anagrafici e valorizzando la password e la domanda e risposta segreta per recupero identità.

Di seguito le URL dell'applicazione WEB dedicata alla gestione delle credenziali:

AMBIENTE ELABORATIIVO	Indirizzo Internet (URL)
TEST (alias certificazione)	https://cert<applicazione>.<dominio>.it
PRODUZIONE (alias esercizio)	https://<applicazione>.<dominio>.it

All'utente è richiesto di inserire la propria CNS nell'apposito lettore e scegliere la prima opzione :

[1]**NOTA**: 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.**

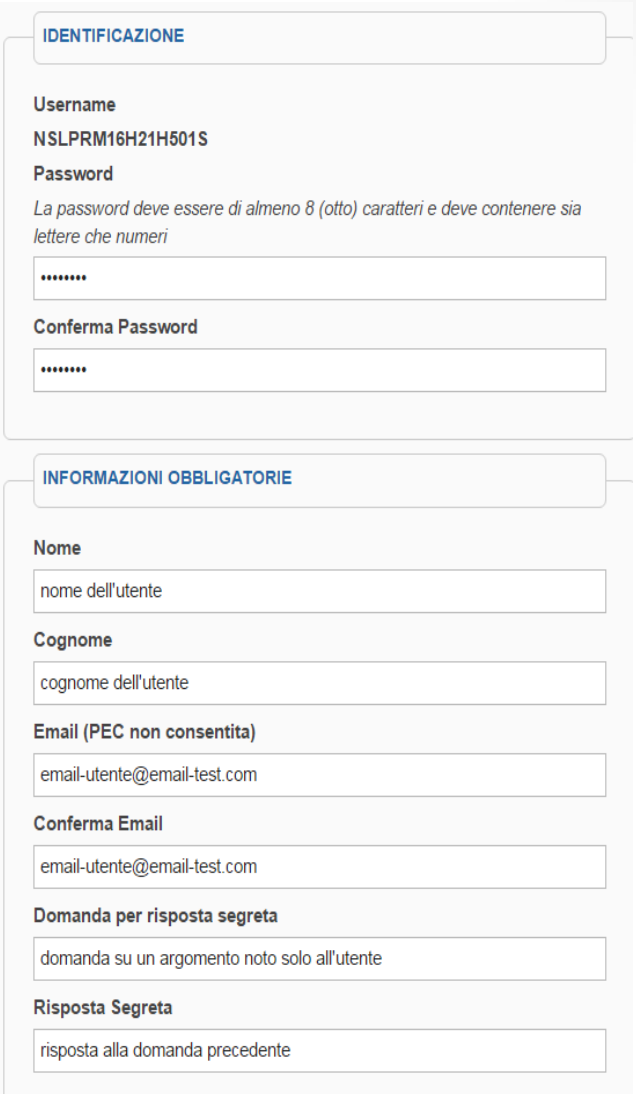
Per i dettagli tecnici e normativi si rimanda al sito AGID:

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

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

All'attivazione del link l'utente è ridiretto sull'applicazione di registrazione dei dati di identificazione, i parametri richiesti sono tutti obbligatori e hanno l'obiettivo di generare un profilo utente con i dati necessari alla sua successiva identificazione.

La ***username*** è valorizzata automaticamente con il **CODICE FISCALE** che è estratto dal campo ***subject*** del certificato di autenticazione presente sulla CNS. La ***username*** potrà essere utilizzata successivamente come credenziale di autenticazione sulle altre applicazioni esposte dal sistema sul canale Internet, applicazioni che richiedano solo la coppia di credenziali *username* e *password.*

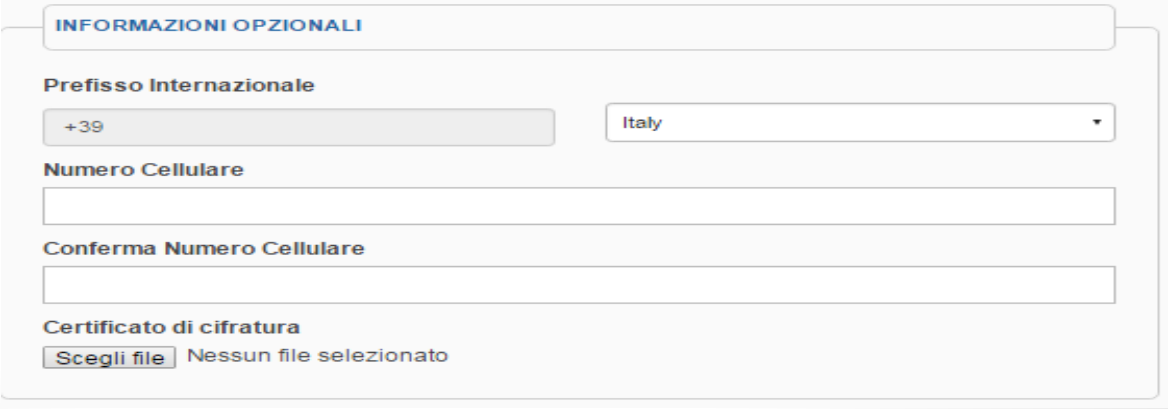


I seguenti parametri sono tutti **obbligatori:**

- ***Password***: deve essere di almeno 8 (otto) caratteri e deve contenere sia lettere che numeri;
- **Nome**;
- **Cognome**;
- **Email**: deve essere fornita un'email valida ai fini della validazione della nuova utenza. **L'indirizzo email non deve essere già presente sul sistema di identificazione** in quanto potrà essere utilizzato per identificare l'utente nei workflow di recupero credenziali.
- **Domanda** e **risposta segreta**: campi di testo ad immissione libera, sono necessari per il recupero completo delle credenziali.

Successivamente l'utente potrà inserire altri parametri **opzionali**:

- **Numero di telefono cellulare**: **potrà** essere utilizzato come **presidio di sicurezza aggiuntivo** in alcune fasi di riconoscimento per il tramite di invio di SMS contenenti codici di sicurezza utilizzabili una sola volta, i cosiddetti OTP (One Time Password).



- **Certificato di cifratura personale**: In tale contesto l'utente **potrà** fornire un certificato x509 di cifratura **personale** che sarà utilizzato solo per cifrare messaggi diretti alla persona fisica identificata dal codice fiscale presente sulla CNS. **Tale certificato non deve essere confuso con il certificato di cifratura associato alla credenziale applicativa (A2A) illustrata nel seguito del documento**.

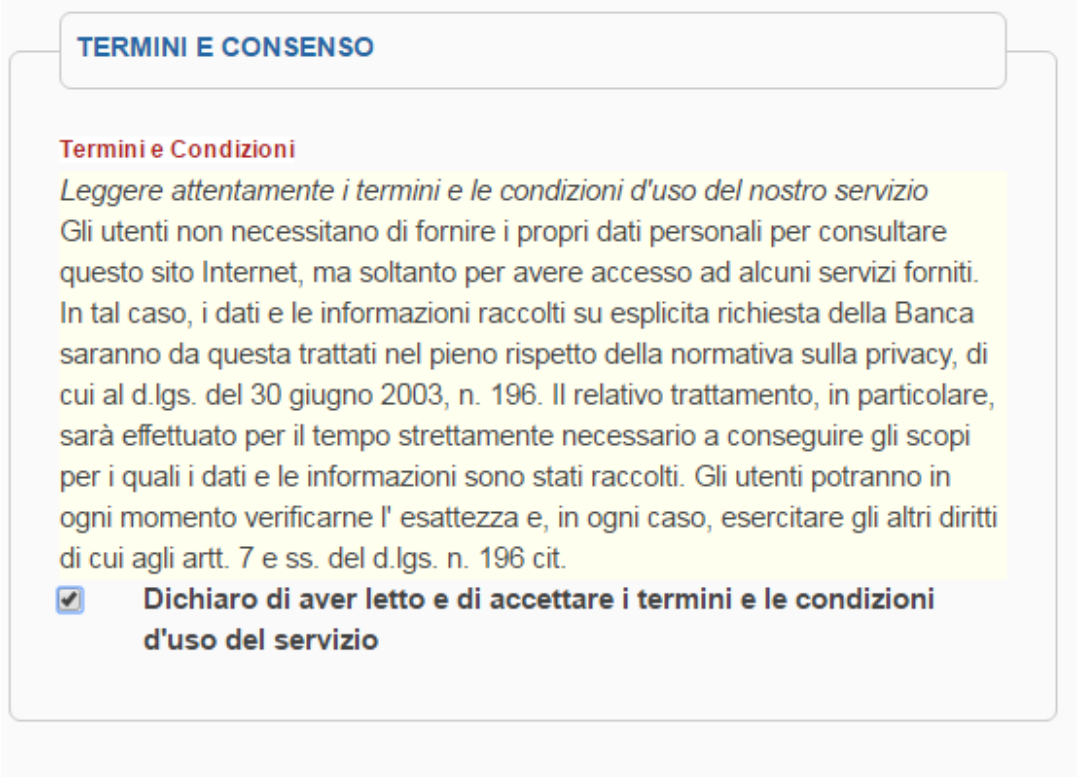
Il certificato di cifratura personale potrà essere sottoposto **in uno dei seguenti formati:**

DER - formato binario

PEM - formato base64

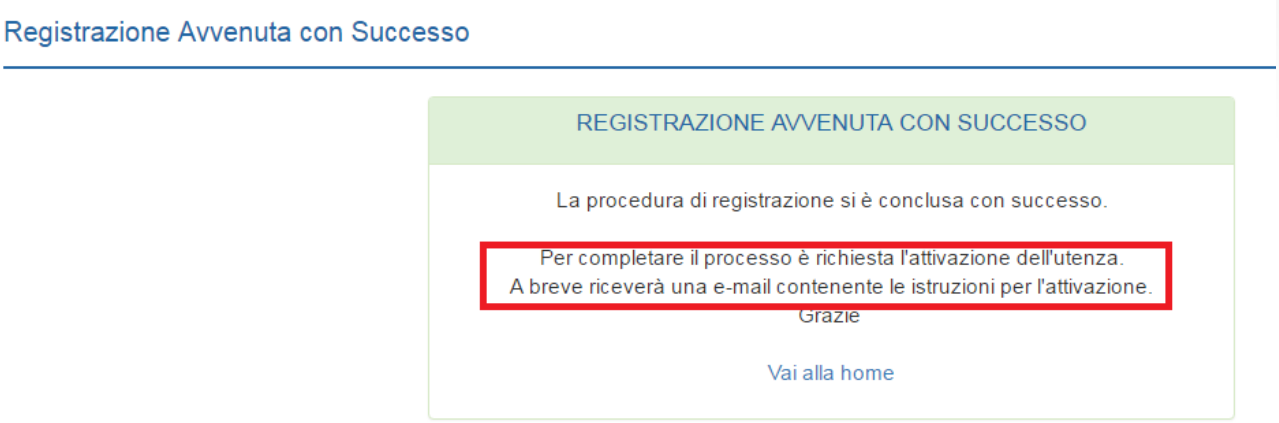
Nel caso in cui il certificato sia firmato da una o più CA intermedie, i certificati di quest'ultime non dovranno essere incluse nel *file* caricato.

Al termine l'utente **dovrà** accettare i termini e le condizioni d'uso del servizio.

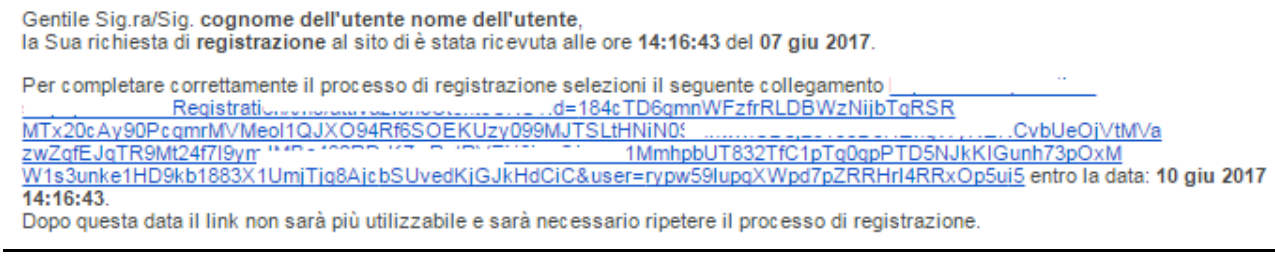


Successivamente alla conferma **il sistema invia una email all'indirizzo indicato in fase di registrazione. Al fine di completare e validare l'iscrizione l'utente dovrà seguire le istruzioni contenute nella stessa email entro 72 ore.**

All'utente è mostrata la seguente schermata:

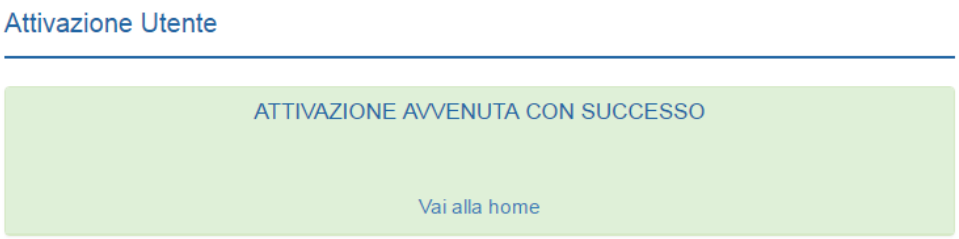


Di seguito un **esempio** di e-mail inviata dal sistema di registrazione:


Gentile Sig.ra/Sig. **cognome dell'utente nome dell'utente**,
la Sua richiesta di **registrazione** al sito di è stata ricevuta alle ore **14:16:43** del **07 giu 2017**.

Per completare correttamente il processo di registrazione selezioni il seguente collegamento
Registrati...d=184cTD6gmnWFzfrRLDBWzNijbTqRSR
MTx20cAy90PcgmrMVMeol1QJXO94Rf6SOEKUzy099MJTSLtHNiN0...CvbUeOjVtMVa
zwZqfEJqTR9Mt24f7l9ym...1MmhpbUT832TfC1pTq0qpPTD5NJkKIGunh73pOxM
W1s3unke1HD9kb1883X1UmjTjq8AjcbSUvedKjGJkHdCiC&user=rypw59lupqXWpd7pZRRHrl4RRxOp5ui5 entro la data: **10 giu 2017 14:16:43**.
Dopo questa data il link non sarà più utilizzabile e sarà necessario ripetere il processo di registrazione.

Cliccando il link contenuto nell'email, l'utente sarà ridiretto su una pagina web che attesterà il completamento dell'attivazione:



Nel caso in cui il link non fosse selezionato entro 72 ore dall'iscrizione, il profilo utente è cancellato definitivamente dagli archivi del sistema e **sarà necessario procedere con una nuova procedura di registrazione**, anche utilizzando gli stessi dati .

In caso di conferma positiva, entro le 72 ore, l'utente sarà abilitato e potrà procedere all'autenticazione della procedura di gestione delle credenziali applicative (A2A):

NOTA: L'utente **che abbia già registrato la propria CNS** scegliendo l'opzione

otterrà dal sistema il seguente messaggio e potrà scegliere tra la funzione di gestione del proprio profilo o accedere direttamente alla gestione delle credenziali applicative.

NOTA : Non è possibile utilizzare un indirizzo e-mail già utilizzato in precedenza per registrare altre credenziali. Qualora non fosse possibile utilizzare un altro indirizzo email o un alias dello stesso, è possibile richiedere la cancellazione delle vecchie credenziali inviando un'email all'indirizzo del *Service Desk.*

Credenziali applicative A2A

L'utente digita la URL dell'applicazione:

AMBIENTE ELABORATIIVO	Indirizzo Internet (URL)
TEST (alias certificazione)	https://cert<applicazione>.<dominio>.it
PRODUZIONE (alias esercizio)	https://<applicazione>.<dominio>.it

e viene ridiretto sul menu di scelta delle azioni relative all'autenticazione e alla **gestione delle credenziali** utente e **A2A:**

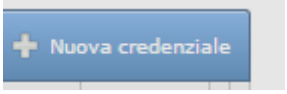
Scegliendo l'opzione "**Gestione delle credenziali applicative**" si accederà alle relative funzionalità di gestione delle credenziali A2A.

Aggiunta nuova credenziale

Ogni utente può registrare un numero illimitato di credenziali delle quali diventa "**manager**".

Ogni credenziale deve **disporre di almeno un certificato digitale** (x509) tra quello con le finalità di autenticazione A2A e quello utilizzabile per la cifratura dei messaggi inviati dal sistema alla controparte (che detiene la chiave privata di cifratura).

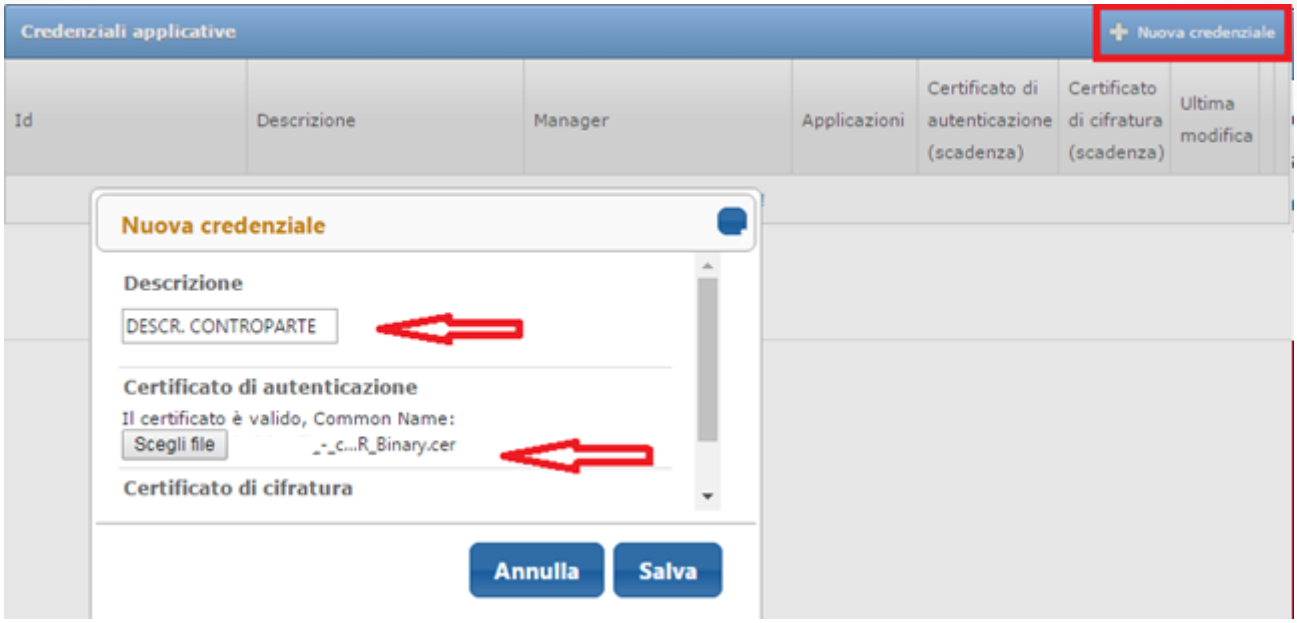
L'aggiunta di una credenziale applicativa (A2A) inizia con la selezione del tasto:



Che avvia la fase di immissione di una nuova credenziale, le informazioni obbligatorie sono

- **Descrizione**: campo di testo libero, si consiglia l'inserimento nome della controparte/ dell'ente/tesoriere/tramite/controparte che richiede le credenziali.

- **Uno o entrambi** i certificati x509 di autenticazione e cifratura



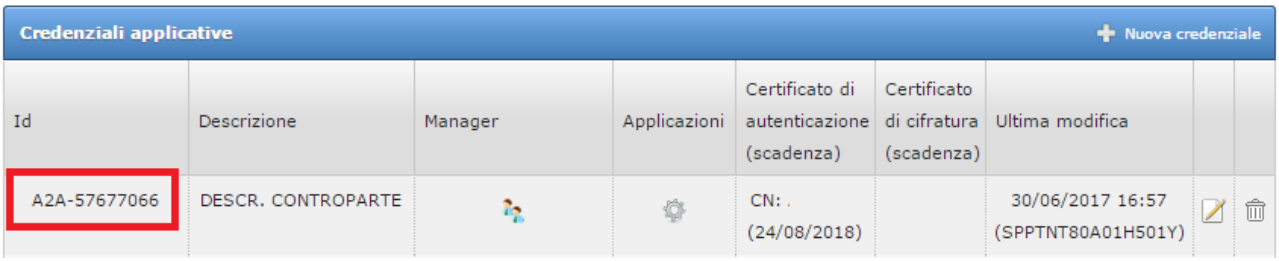
Il certificati X509 potranno essere sottoposti **in uno dei seguenti formati:**

DER - formato binario

PEM - formato base64

Nel caso in cui il certificato sia firmato da una o più CA intermedie, i certificati delle CA intermedie o radice **non devono** essere incluse nel *file* caricato.

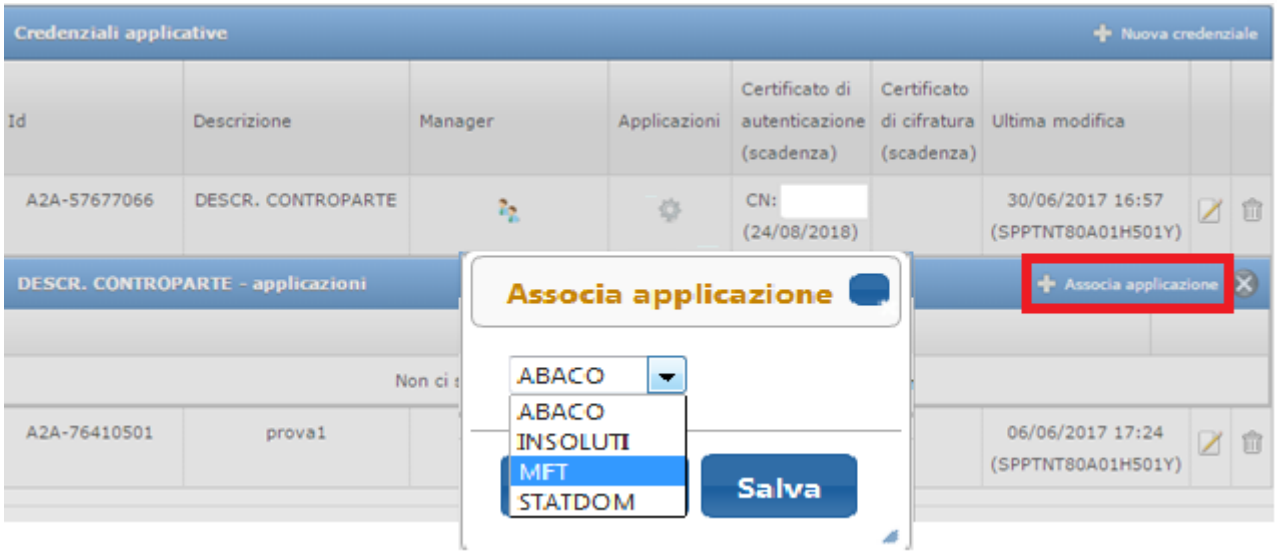
Una volta completata l'immissione delle informazioni richieste, **il sistema genera automaticamente un ID che identifica univocamente la credenziale applicativa.**



Gestione dell'abilitazione all'applicazione.

Ogni credenziale permette di fare riferimento ad un certificato di autenticazione e/o di cifratura per una o più applicazioni esposte su Internet dal sistema.

Al momento della creazione la credenziale viene memorizzata **ma non abilitata ad alcuna applicazione, tale azione deve essere espressamente richiamata da un utente manager della stessa credenziale**:

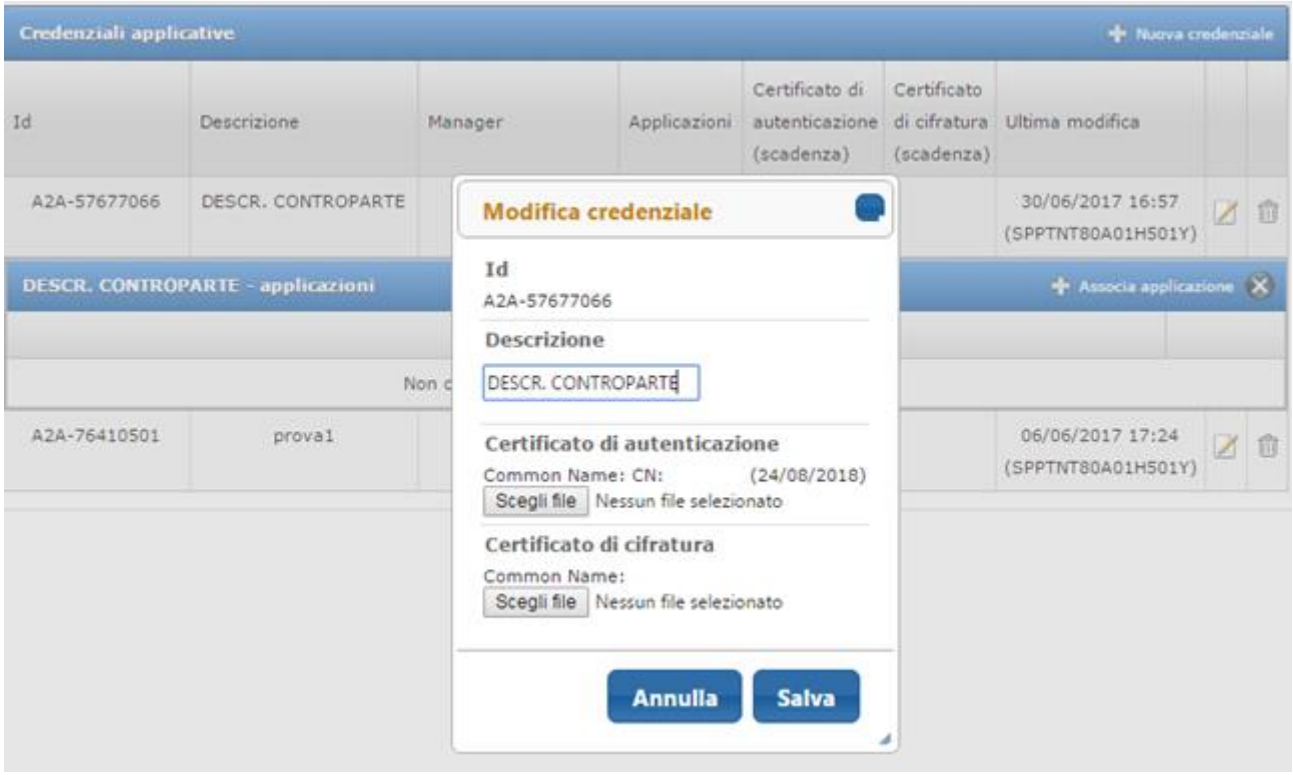


Al fine di permettere l'abilitazione sui sistemi di autenticazione è necessario cliccare sull'azione "**+ Associa applicazione**" , tale azione permetterà l'associazione ad una delle applicazioni.

NOTA: Una credenziale può essere abilitata a diverse applicazioni che potranno essere rese disponibili nel tempo. Un manager può gestire le abilitazioni di credenziale per una qualunque applicazione in qualsiasi momento. La disabilitazione è ottenuta attraverso la funzione "cestino"

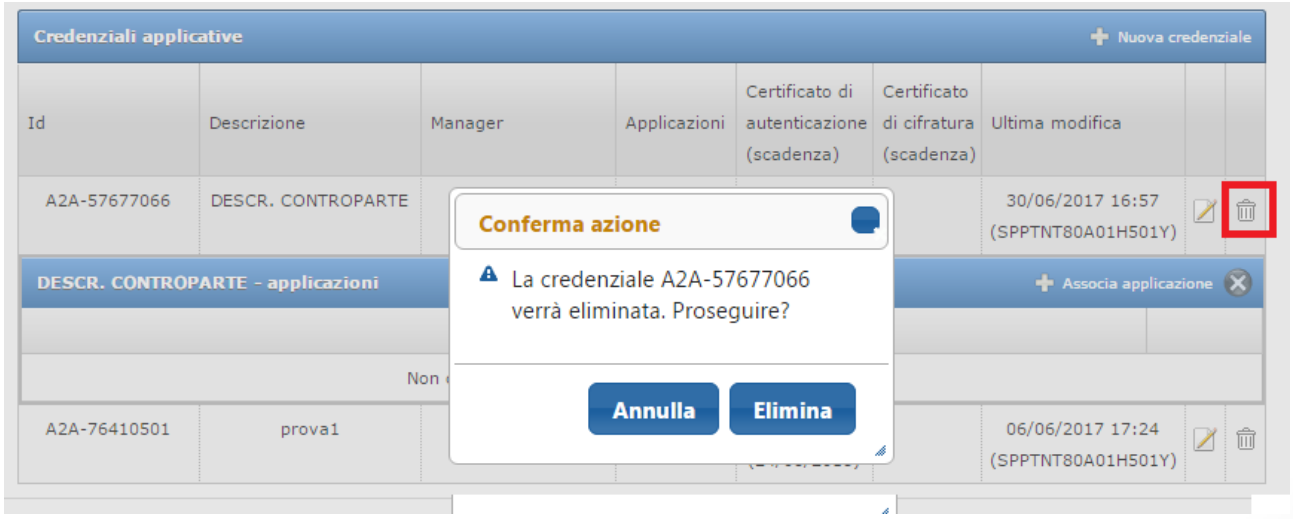
Modifica della credenziale

I ***manager*** possono in ogni momento **variare la descrizione** e **sostituire** i certificati di autenticazione e cifratura della credenziale.



Cancellazione della credenziale

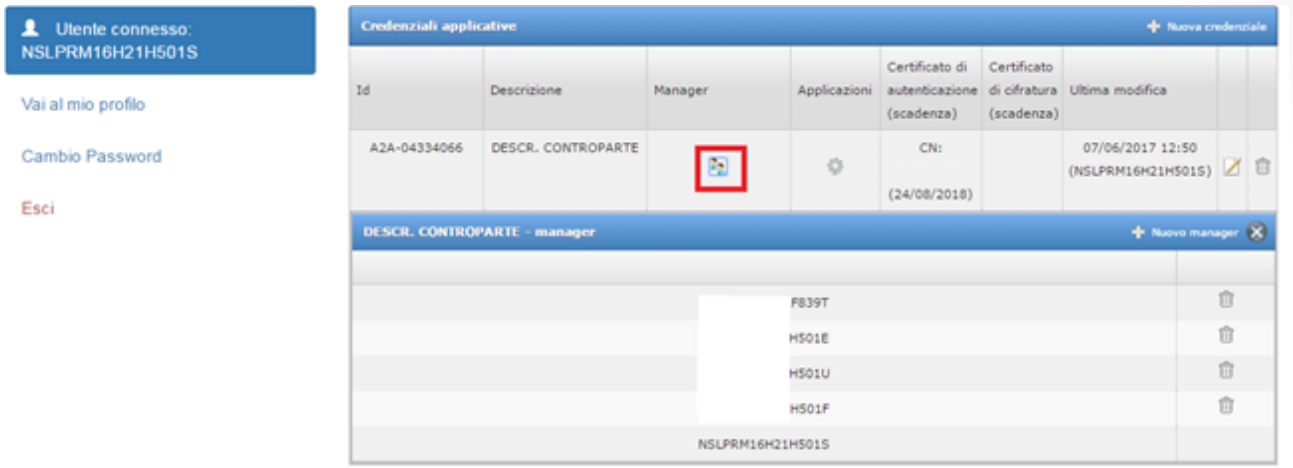
Un manager può in qualunque momento cancellare una credenziale, **l'eliminazione non può essere annullata** e non è possibile riutilizzare lo stesso codice identificativo di una credenziale cancellata (Id). La cancellazione può essere effettuata direttamente nella maschera di gestione delle credenziali applicative come mostrato nella figura seguente:



Gestione del manager della credenziale

Una credenziale può essere gestita da un numero illimitato di *manager.*

È possibile visualizzare **l'elenco dei manager** di una credenziale cliccando sull'icona evidenziata nella figura seguente:



Uno qualunque dei manager può delegare la gestione della credenziale ad altri manager inserendo il **codice fiscale** dei nuovi manager.

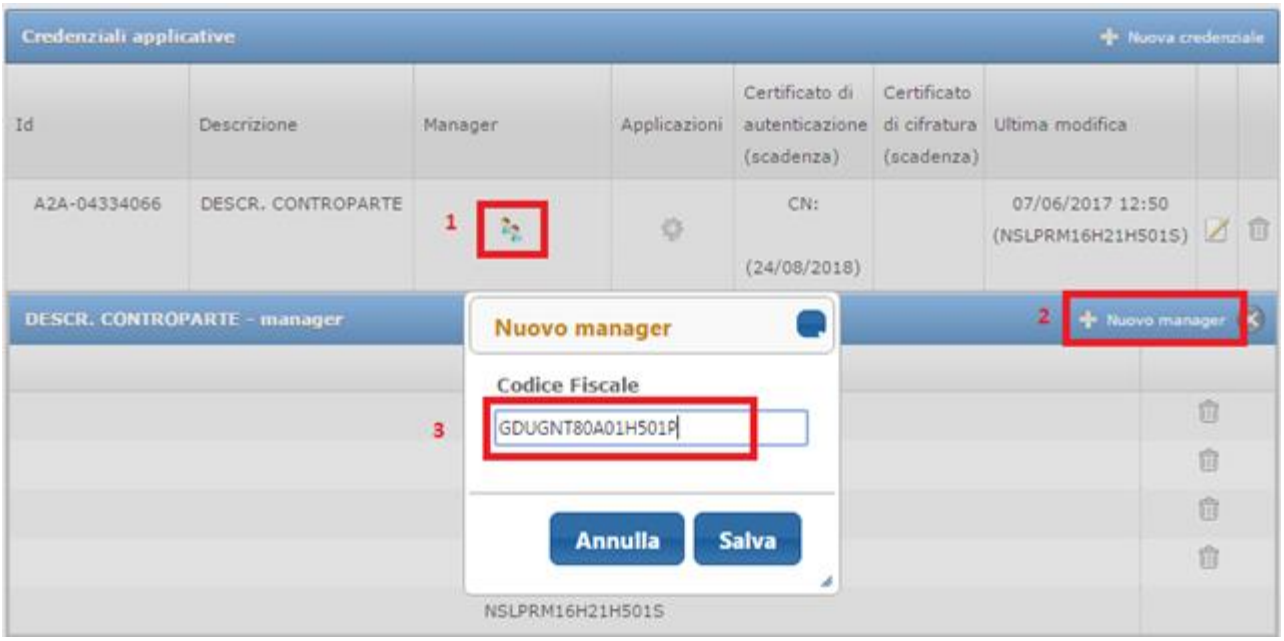
La **delega** di gestione non è esclusiva, tutti i manager possono operare sulle proprie credenziali sfruttando tutte le funzionalità associate.

Un qualunque manager può eliminare un altro manager dalla gestione della credenziale, tale operazione non ha effetto sulle altre credenziali applicative ad esso associate e non ha effetto sulla credenziale associata alla CNS del manager eliminato.

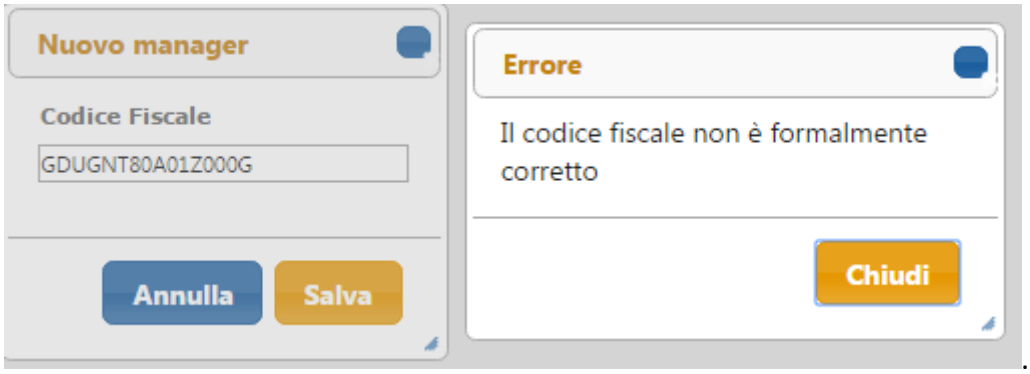
Delega ad un nuovo manager

La gestione non esclusiva di una credenziale applicativa può essere delegata tra i diversi manager.

Il meccanismo di delega si basa sulla comunicazione al sistema del CODICE FISCALE del nuovo manager attraverso l'interfaccia di gestione della credenziale, come mostrato nella figura sottostante:



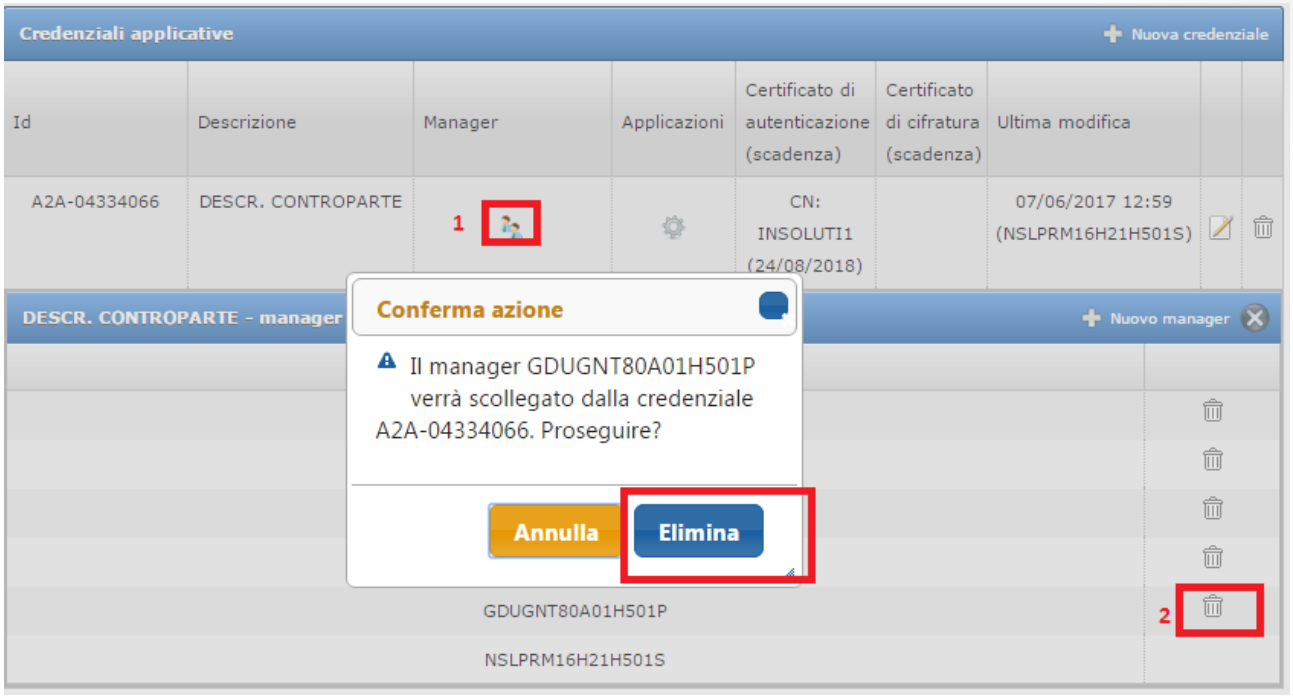
NOTA: L'aggiunta del codice fiscale di un manager può essere condotto a termine ancor prima della sua iscrizione; il sistema **verifica solo la correttezza formale** del codice fiscale inserito:



.

Cancellazione di un manager

Il nuovo manager può gestire anche gli altri manager, eventualmente **eliminando i manager** non più necessari, di seguito un esempio:



Alla conferma dell'azione il manager selezionato sarà scollegato dalla credenziale applicativa; tale azione non influisce sullo status dell'utente che viene scollegato dalla credenziali che continua a mantenere il ruolo di manager di tutte le altre credenziali a lui associate.

NOTA: una credenziale non può rimanere "orfana" quindi ogni manager può eliminare tutti i manager escluso se stesso.

In caso di necessità di cancellazione e/o modifica urgente o massiva è tuttavia possibile richiedere il supporto gestionale da parte del service-desk, in particolare in caso di incidenti di sicurezza.

FAQ

CNS

1. Cos è la CNS?

La Carta Nazionale dei Servizi (CNS) è lo strumento attraverso il quale i cittadini vengono riconosciuti in rete in modo certo. 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 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*?

Deve essere in possesso di una CNS con il suo lettore oppure 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 alcuni 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 seguito la guida di installazione del software a corredo della CNS (driver) del fornitore del carta CNS. Accertarsi 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.

REGISTRAZIONE

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.

CREDENZIALI APPLICATIVE E CERTIFICATI DIGITALI

10. Cosa 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. 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 .

12. Centri servizi/Tramite Ente/Tramite Tesoriere - È possibile per un centro servizi utilizzare un unico certificato di autenticazione di proprietà del centro servizio?

Per accedere al servizio di trasferimento flussi su internet ciascun segnalante deve dotarsi di una propria credenziale applicativa. Nel caso in sui i segnalanti siano intermediati da uno o più Centri Servizi questi potranno utilizzare una credenziale applicativa di loro proprietà.

13. Centri servizi/Tramite Ente/Tramite Tesoriere - Nel caso in cui un centro servizi svolga operazioni di scambio per conto di più segnalanti, dovrà utilizzare una credenziale differente per ogni segnalante?

In generale il centro servizi potrà utilizzare lo stesso certificato di autenticazione abilitato per lo specifico contesto applicativo per veicolare tutti i messaggi (flussi dati) dei propri clienti (segnalanti intermediati).

14. Centri servizi/Tramite Ente/Tramite Tesoriere - 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 e 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 atraverso il portale informativo.

Per i messaggi trasmessi dal sistema e il cui destinatario è un intermediario: esisterà un certificato di cifratura caricato sulla credenziale A2A associato all'intermediario.

15. Gestione dei certificati digitali - 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.

16. Formato dei certificati digitali - 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)

17. Tipologia dei certificati

-- ***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.*

18. 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.*

19. Acquisto dei certificati digitali - 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 il cui certificato ROOT sia presente nel CA_BUNDLE della fondazione Mozilla e consultabile al link:*

https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/

20. Cifratura - 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.

21. 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.

AUTENTICAZIONE APPLICATIVA (A2A)

22. Come si usa il certificato X509 di autenticazione

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

23. 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 ha firmato il certiificato SSL del SERVER che eroga le funzionalità applicative.

24. 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
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.*