

**SPID**

**RELAZIONE TECNICA**

Livello di sicurezza del sistema di autenticazione informatica

Controlli e Procedure di conformità per il servizio di autenticazione SPID

|  |  |
| --- | --- |
| *Versione:* | *1.0* |
| *del:* | 06/09/2015 |

# Indice degli argomenti

1 Indice degli argomenti 2

2 Riferimenti 3

3 Scopo del Documento 4

3.1 Basic Authentication 4

3.2 One Time Password via SMS (Livello SPID 2, LoA 3) 4

3.3 Time Based One Time Password (Livello SPID 2, LoA 3) 5

3.4 Mutua autenticazione TLS (Livello SPID 3, LoA 4) 6

4 Gestione delle credenziali 7

4.1 Premessa 7

4.2 Credenziali di Livello 1 SPID (LoA2) 7

4.2.1 Descrizione 7

4.2.2 Consegna 8

4.3 Credenziali di Livello 2 SPID (LoA3) 8

4.3.1 Descrizione OTP via SMS 8

4.3.2 Consegna OTP via SMS 8

4.3.3 Descrizione OTP via App 8

4.3.4 Consegna OTP via App 8

4.4 Credenziali di Livello 3 SPID (LoA4) 9

4.4.1 Descrizione 9

4.4.2 Consegna 9

5 Autenticazione 10

5.1 Premessa 10

5.2 Meccanismi di autenticazione informatica a Livello 1 SPID (LoA2) 10

5.3 Meccanismi di autenticazione informatica a Livello 2 SPID (LoA3) 10

5.3.1 Descrizione OTP via SMS 10

5.3.2 Descrizione OTP via App 11

5.4 Meccanismi di autenticazione informatica a Livello 3 SPID (LoA4) 11

# Riferimenti

1. Decreto del Presidente del Consiglio dei Ministri 24 ottobre 2014 (Gazzetta Ufficiale N. 285 del 9 Dicembre 2014). “Definizione delle caratteristiche del sistema pubblico per la gestione dell’identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese” .
2. Regolamento recante le modalità per l’accreditamento e la vigilanza dei gestori dell’identità digitale (art. 1, c. 1, lett. l), DPCM 24.10.2014)” http://www.agid.gov.it/sites/default/files/circolari/regolamento\_accreditamento\_v1.pdf - pubblicato sul sito istituzionale dell’Agenzia (28 luglio 2015)
3. Determinazione n. 44/2015 - AGID (28 luglio 2015)
4. Regolamento recante le regole tecniche (articolo 4, comma 2, DPCM 24 ottobre 2014) <http://www.agid.gov.it/sites/default/files/circolari/spid-regole_tecniche_v1.pdf> - pubblicato sul sito istituzionale dell’Agenzia (28 luglio 2015)
5. Regolamento modalità attuative <http://www.agid.gov.it/sites/default/files/circolari/spid-modalita_attuative_v1.pdf> - pubblicato sul sito istituzionale dell’Agenzia (28 luglio 2015)
6. MG605 - Politiche di sicurezza POL/A9\_PASWD -  Password, Credenziali e strumenti di Autenticazione
7. SPID Provisioning -ST– Specifiche Tecniche– Versione 1.1.0 del 18/08/2015
8. ISO/IEC 29115:2013 ISO/IEC 29115:2013

# Scopo del Documento

Questo documento illustra le procedure implementate per il servizio di autenticazione parte del sistema federato denominato SPID. Il sistema fornisce diverse opzioni (meccanismi di autenticazione, con diversi livelli di attendibilità) e per ognuno di questi saranno presentati gli accorgimenti tecnici adottati in conformità con le regole adottate dal gruppo di lavoro di AgID per il soddisfacimento dei requisiti della ISO/IEC 29115. In sintesi la relazione tecnica intende dimostrare il livello di sicurezza, secondo quanto stabilito dall’art. 6, comma 1 del DPCM, da parte di ciascun modulo di autenticazione realizzato da InfoCert relativamente ai rispettivi Livelli SPID.

Il documento quindi illustrerà le caratteristiche di 4 metodi di autenticazione, descritti nel seguito, denominati:

1. Basic Authentication (Livello SPID 1, LoA 2)
2. One Time Password via SMS (Livello SPID 2, LoA 3)
3. Time Based One Time Password (Livello SPID 2, LoA 3)
4. Mutua autenticazione TLS (Livello SPID 3, Loa 4)

## Basic Authentication

Il metodo implementa una soluzione con livello SPID 1 (LoA 2) ed utilizza come credenziali per l’autenticazione una coppia username/password che viene assegnata all’utente in fase di emissione. Pertanto la modalità di autenticazione è a singolo fattore tramite richiesta di inserimento da parte dell’utente delle credenziali assegnate: [UserID/mail/PEC] + [password].

Le modalità di assegnazione delle credenziali sono tutte quelle descritte nel documento di specifiche tecniche di provisioning SPID InfoCert [7] , già validate fino al LoA 4 [i*.e. in-person identity proofing for human entities o de-visu*].

La password deve rispettare le policy definite da InfoCert come descritto nel documento [“POL/A09\_PASWD - Password, Credenziali e strumenti di Autenticazione”]. Per maggiore chiarezza si riportano nel seguito i vincoli elementari che devono essere soddisfatti:

* DEVE essere almeno di lunghezza 8 caratteri.
* DEVE contenere almeno un carattere alfabetico ed uno numerico.
* non DEVE contenere più di due caratteri identici consecutivi.
* non DEVE essere simile alla password precedente.
* non DEVE contenere l’user-id come parte della password.
* non DEVE essere riconducibile ai dati anagrafici dell’incaricato o di suoi familiari.
* non DEVE essere riconducibile a marchi o a nomi di prodotto.

Tutte le password devono essere cambiate almeno ogni 6 mesi a cura degli incaricati (titolari delle credenziali) ovvero ogni 3 mesi nel caso di accesso a dati sensibili ai sensi della normativa in materia di privacy.

Sono attivi meccanismi proattivi per la gestione della scadenza del periodo di validità (expiration) password (messaggi avvisano l’utente prima della scadenza del periodo di validità della password o prima che venga definitivamente disabilitata).

Analogamente quando l’utente sceglie la prima password o modifica la password iniziale una procedura automatica garantisce l’applicazione delle policy descritte precedentemente.

Tutto il protocollo per l’autenticazione con l’IdP avviene secondo le specifiche del protocollo SAML 2.0 come descritto nell’RFC 6595 dell’ Internet Engineering Task Force (IETF) ISSN: 2070-1721 dell’ Aprile 2012 e secondo le specifiche di interfaccia SPID definite da AGID.

## One Time Password via SMS (Livello SPID 2, LoA 3)

Questa modalità di autenticazione prevede che in fase di emissione l’utente associ al proprio profilo un numero di telefono mobile capace di ricevere SMS. Quando l’IdP riceve una richiesta di autenticazione per un utente, dopo aver provveduto ad una autenticazione di primo livello (nel caso possegga già un token di autenticazione valido non sarà necessario l’inserimento di ulteriori dati), il sistema provvederà alla generazione di un numero casuale di 8 cifre che verrà inviato all’utente via SMS.

L’OTP generato avrà una durata limitata nel tempo e sarà associato alla specifica richiesta tramite una chiave alfanumerica posta davanti all’OTP che verrà visualizzata al momento della richiesta dell’OTP da parte dell’IdP. Il prefisso ha anche lo scopo di evitare attacchi di fishing. Infatti al momento della richiesta del codice l’autenticatore dovrà dimostrare di conoscere il prefisso visualizzando l’informazione nella form di login.

Le modalità di assegnazione delle credenziali sono tutte quelle descritte nel documento di specifiche tecniche di provisioning SPID InfoCert [7] , già validate fino al LoA 4 [i*.e. in-person identity proofing for human entities o de-visu*].

In maniera proattiva in fase di emissione l’IdP dovrà verificare la validità del numero di cellulare associato all’utente inviando una challange (ancora un numero casuale di 8 cifre) che dovrà essere inserita in una apposita form.

Analogamente sono state previste le procedure di gestione della ~~emissione per la~~ modifica del numero di cellulare.

Il metodo utilizza due fattori distinti: le credenziali di autenticazione necessarie per avviare il protocollo, ed il possesso della SIM telefonica (e del relativo PIN se presente) che abilita il numero telefonico associato all’utente.

Nel seguito saranno descritti tutti gli accorgimenti adottati sia in fase di consegna delle credenziali che in fase di esercizio ordinario per poter classificare il servizio conforme alle specifiche Livello SPID 2 LoA 3.

## Time Based One Time Password (Livello SPID 2, LoA 3)

InfoCert ha sviluppato una sistema di generazione di OTP per dispositivi mobili basati su iOS e Android che rispetta le specifiche descritte nella RFC 6238 dell’Internet Engineering Task Force (IETF) ISSN: 2070-1721 del Maggio 2011.

Il metodo è basato su un’estensione dell’algoritmo per la generazione di One Time Password basato su funzione HMAC (anche esso definito nella RFC 4226) per aggiungere al calcolo un fattore legato al tempo corrente.

In sintesi il sistema a partire da un algoritmo noto che calcola la funzione HMAC (funzione di hash con chiave, definita dall’IETF nell’RFC 2104) ed un seme (definito seed nel seguito) condiviso (tra l’App dell’utente ed il modulo autenticatore dell’IdP di lunghezza 512 bit), calcola l’hash dell’ora corrente espressa in secondi dal 1 gennaio 1970 (cosiddetto Unix Time) opportunamente arrotondato per avere una finestra di ampiezza predefinita, utilizzando il seme come chiave (quantità di sicurezza).

Per evitare attacchi che possano riutilizzare l’OTP, la finestra di validità del token sarà tenuta intenzionalmente molto stretta (minore di 30 secondi secondo le raccomandazioni dell’RFC 6238), ma sufficientemente ampia per tollerare i ritardi della rete o introdotti dall’utente. In altri termini l’ora corrente sarà arrotondata eliminando le cifre meno significative secondo “Time-Step” di ampiezza pari a 30 secondi.

Il server provvederà a verificare l’OTP ricevuto con una sequenza di valori generati localmente in una finestra ampia a piacere (fino a 600 secondi).

La sincronizzazione tra la device mobile ed il server dell’IdP sarà garantita attraverso l’utilizzo di server NTP o semplicemente abilitando sensori GPS sempre più disponibili sulle device mobili.

Il seme, generato al momento dell’emissione utilizzando l’output di una funzione di hash quale SHA-512 (64 byte), sarà memorizzato sulla device mobile cifrato con AES, utilizzando un PIN scelto dall’utente. Il PIN dovrà essere inserito dall’utente ad ogni utilizzo o sarà legato allo screensaver del dispositivo.

Per la fase di emissione è stato previsto un protocollo on-line che utilizza prima le credenziali utilizzate per la basic authentication, successivamente una challange inviata via SMS ed infine una primo OTP generato dall’App.

L’implementazione rispecchia fedelmente i parametri introdotti nella reference implementation descritta dalle RFC di riferimento ereditando quindi tutti i risultati delle analisi sulla sicurezza dei valori generati che dimostrano matematicamente che i valori risultanti sono uniformemente distribuiti ed indipendenti tra loro.[RFC4226].

Questo meccanismo di autenticazione utilizza due fattori distinti: i dati noti all’utente (username e PIN) ed una quantità di sicurezza opportunamente custodita dal dispositivo in possesso dell’utente (secondo fattore) su cui viene installata l’App. Meccanismi analoghi vengono adottati con token fisici, la cui robustezza ad attacchi esterni non è stata ancora dimostrata. Nel seguito saranno descritti tutti gli accorgimenti adottati sia in fase di consegna delle credenziali che in fase di esercizio ordinario per poter classificare il servizio conforme alle specifiche Livello SPID 2 LoA 3.

## Mutua autenticazione TLS (Livello SPID 3, LoA 4)

Durante la sperimentazione è stato realizzato anche un meccanismo di autenticazione conforme alle specifiche Livello 3 SPID o (Loa 4). Il sistema utilizza il certificato X.509 presente sulla carta nazionale dei servizi (CNS) per attivare il protocollo TLS con mutua autenticazione. In questo caso, dopo che l’utente ha inserito il PIN corretto, al termine del protocollo l’IdP riceve le informazioni contenute nel certificato, tra cui il campo Canonical Name con l’identità dell’utente / codice fiscale. Dopo aver verificato la validità del certificato, l’IdP utilizza il serial number del certificato per identificare l’utente nel proprio user store.

Il sistema è stato testato utilizzando il browser mozilla/firefox.

Questo meccanismo di autenticazione utilizza due fattori (il PIN noto all’utente ed il possesso della smart card che contiene il certificato). Inoltre la chiave privata presente sulla smart card viene custodita da un dispositivo tamper proof già certificato per gli usi previsti. Pertanto risponde alle specifiche citate come Livello SPID 3 LoA 4.

# Gestione delle credenziali

## Premessa

La fase di **gestione delle credenziali** comprende tutti i processi relativi alla gestione del ciclo di vita di una credenziale. Alcuni di questi processi dipendono dal fatto se le credenziali sono trasportate o meno su un dispositivo hardware.

Il processo di ***emissione*** delle credenziali è il processo di fornire o in altri termini di associare una identità digitale con una credenziale: alla convalida della procedura di Registrazione, il sistema del Gestore crea e personalizza le credenziali assegnate al Richiedente (che sono in uno stato non attivo per motivi di sicurezza).

Il processo di ***consegna*** rappresenta l’ultima fase relativamente al processo di rilascio di una identità digitale: la complessità varia con il livello di Assurance (LoA) necessario.

In questo paragrafo saranno descritte le procedure di emissione e consegna delle credenziali per i 3 sistemi di autenticazione:

* Username / Password
* Associazione del numero del cellulare per quanto riguarda l’invio di OTP via SMS
* Generazione e condivisione del segreto (seed) per quanto riguarda l’utilizzo di un App per la generazione di OTP attraverso un generatore di numeri casuali

## Credenziali di Livello 1 SPID (LoA2)

### Descrizione

**DESCRIZIONE DEL processo già utilizzato per l’assegnazione di username e password**

Vedi documento elvio – Provvisioning SPID 5.1; 5.2

Il processo prevede la scelta da parte del titolare dei dati d'accesso userid, password e l'indirizzo email principale attraverso un portale che propone l'inserimento della userid, della password (con la conferma) e dell'email ; questi campi sono tutti obbligatori.

Il portale verifica che:

* la userid sia univoca per i sistemi InfoCert
* la password segua le policy di SPID
  + la lunghezza deve essere minima di 8 caratteristica
  + vi devono essere lettere maiuscole e minuscole
  + vi deve essere l'inclusione di uno o più caratteri numerici
  + non deve contenere più di due caratteri consecutivi
  + vi deve essere incluso un carattere speciale (#,$,%, ecc.)
  + deve avere una durata massima non superiore a 180 giorni
  + non possono essere riusate prima di 5 e comunque non prima di 15 mesi.
* l’indirizzo e\_mail sia univoco
  + non sia già presente nei sistemi InfoCert
  + non sia presente nel mondo SPID

Per verifica positiva i dati vengono registrati e quindi il portale visualizza la notifica dell’invio di un messaggio alla casella e\_mail indicata in fase di registrazione e che l’invito a proseguire utilizzando il link indicato nel testo del messaggio ricevuto.

Il sistemi di gestione delle credenziali utenti InfoCert [ISAC] inserisce la entry della userid (nickname) e password qualificate solo per rientrare nella registrazione o nel sito di attivazione per il completamento della registrazione.

### Consegna

**DESCRIZIONE DEL PROCESSO DI CONSEGNA DELLE CREDENZIALI**

Vedi documento elvio – Provvisioning SPID 5.1; 5.2

L'esecuzione del link personalizzato permette di verificare l’indirizzo email dichiarato in fase di registrazione, la possibilità di modifica password e il completamento della registrazione utente.

Il link personalizzato è attivo per 30 giorni; alla scadenza del periodo il sistema provvede all’annullamento della registrazione non completata entro 30 giorni.

Il sistema manda quindi una email di conclusione processo di registrazione all'indirizzo email principale indicata in fase di registrazione.

## Credenziali di Livello 2 SPID (LoA3)

### Descrizione OTP via SMS

Il sistema descritto associa alle normali credenziali di Livello 1 SPID anche un numero di telefono mobile che sarà abilitato alla ricezione e visualizzazione dell’OTP inviato dal modulo autenticatore dell’IdP.

Il processo assume che non sia possibile presentarsi alla rete telefonica pubblica con un numero di telefono appartenente ad un altro utente. Benchè motivata da solide basi tecniche e suffragata da numerosi documenti dell’ITU (International Telecommunication Union) la dimostrazione di tale proprietà è oltre lo scopo del presente documento pertanto in questo paragrafo sarà descritta solo la fase di associazione del numero di telefono con il profilo utente.

### Consegna OTP via SMS

Attraverso funzioni di selfcare erogate dal portale appositamente realizzato ed abilitate da una autenticazione di livello 1 l’utente provvederà a registrare il numero del cellulare scelto al quale saranno inviati via SMS le OTP generate dall’IdP. Una volta inserito il numero di cellulare l’utente dovrà provare di possedere il numero scelto, inserendo il codice ricevuto come prima attivazione.

Non vi sono altre credenziali.

### Descrizione OTP via App

Per quanto riguarda la generazione di Time Based One Time Password, l’App ed il modulo di autenticazione dell’IdP devono condividere una quantità di sicurezza definita “seed” che viene utilizzata come chiave per il calcolo della funzione HMAC utilizzata per la generazione dei digit che compongono l’ OTP.

Nella versione corrente è stato utilizzato un HMAC che restituisce un valore di 512 bit. Anche il seed iniziale ha la stessa lunghezza e viene generato in maniera casuale al momento dell’attivazione dell’App.

### Consegna OTP via App

L’App, firmata dallo sviluppatore, viene installata direttamente dallo store (Apple Store per i sistemi iOS o Google Store nel caso di Android) di riferimento che ne garantisce l’integrità. Prima di essere utilizzata deve essere eseguita una procedura di enrollment online direttamente con l’IdP.

In sintesi, l’utente utilizza prima le proprie credenziali di Livello SPID 1 per accedere al servizio, successivamente viene identificata la device su cui è installata l’App, attraverso un’autenticazione di livello SPID 2 basata su invio di SMS alla device che deve essere abilitata. Se viene correttamente riconosciuto l’IdP genera un numero casuale di 512 bit che viene inviato su canale cifrato HTTPS (attraverso un servizio REST) all’App.

L’App provvede a memorizzare il seed in un proprio store opportunamente cifrato (per iOS si utilizza il secure store protetto da impronta digitale, per le device che non dispongono di un simile meccanismo, prima di essere salvato, il seed viene cifrato con AES ed una chiave derivata dal pin dell’applicazione di lunghezza 256 bit. Attraverso la gestione delle preferenze dell’utente è possibile configurare l’App affinché chieda il PIN ogni volta che si utilizza il seed (cioè ogni volta che viene generato un OTP) ovvero che il PIN venga tenuto in memoria per tutta la durata dell’esecuzione dell’App richiedendolo solo all’avvio.

Una volta salvato il seed, per completare la procedura viene generato ed inviato il primo elemento della sequenza pseudo casuale, sia per verificare che la procedura è stata correttamente eseguita, sia per calcolare il ritardo di comunicazione dovuto alla rete. Una volta verificato l’OTP ricevuto, se corretto, il server salverà nello user store il seed condiviso con l’utente. In questo caso il seed viene cifrato con la chiave pubblica dell’IdP, utilizzando direttamente l’algoritmo RSA per la cifratura. Pertanto ogni volta che l’IdP dovrà accedere al seed per generare l’OTP lato server sarà necessaria la chiave private dell’IdP attualmente memorizzata su un HSM per ragioni di prestazioni.

## Credenziali di Livello 3 SPID (LoA4)

### Descrizione

Il sistema Sanitario Nazionale, provvede già da tempo, attraverso le regioni, a distribuire la cosiddetta Carta Nazionale dei Servizi, che viene emessa con un tracciato comune in tutto il territorio nazionale, che contiene tra l’altro un certificato X.509 utile per identificare il cittadino.

Pur essendo un meccanismo molto sicuro, la scarsa diffusione dei lettori di smart card ed il fatto che non tutte le regioni italiane hanno messo a disposizione i servizi per l’attivazione (rilascio di PIN e PUK) hanno drasticamente limitato la diffusione della CNS come strumento di autenticazione.

Al contrario sono in aumento di servizi (come l’accesso ai servizi del Ministero di Giustizia, come il Processo Civile Telematico) che prescrivono l’utilizzo della CNS come strumento per l’autenticazione forte (Livello 3 SPID).

### Consegna

Il processo di distribuzione ed attivazione delle CNS è condotto dalle agenzie sanitarie regionali. L’utente in possesso della propria CNS e del relativo PIN (rilasciato all’attivazione) può aggiungere la CNS come strumento di autenticazione sempre attraverso il portale di InfoCert dedicato alle funzioni di autenticazione.

La procedura richiede di firmare un documento casuale con data e ora. Nel verificare la firma, se corretta l’IdP ricava il serial number del certificato ed utilizza questa informazione per collegare il certificato all’identità dell’utente.

# Autenticazione

## Premessa

Il processo di **autenticazione** prevede l'uso di un protocollo per dimostrare il possesso e/o il controllo di una credenziale per stabilire la fiducia in una identità.

I requisiti del protocollo di autenticazione variano a seconda del *Livello di Assurance* (*LoA*) applicabile. L’autenticazione a più fattori è richiesta ai livelli LoA3 e LoA4.

Il processo di verifica delle credenziali utente (l’**autenticazione**) è in grado di assicurare i seguenti livelli di sicurezza:

* **Livello di sicurezza 1 (LoA2 dello standard ISO/IEC 29115)** – sistemi di autenticazione informatica ad un fattore (password o parola chiave);
* **Livello di sicurezza 2 (LoA3 dello standard ISO/IEC 29115)** – sistemi di autenticazione informatica a due fattori, non basati necessariamente su certificati digitali le cui chiavi private siano custodite su dispositivi che soddisfano i requisiti di cui all’Allegato 3 della Direttiva 1999/93/CE del Parlamento europeo;
* **Livello di sicurezza 3 (LoA4 dello standard ISO/IEC 29115)** – sistemi di autenticazione informatica a due fattori basati su certificati digitali, le cui chiavi private siano custodite su dispositivi che soddisfano i requisiti di cui all’Allegato 3 della Direttiva 1999/93/CE del Parlamento europeo.

## Meccanismi di autenticazione informatica a Livello 1 SPID (LoA2)

Quando un utente accede un servizio viene automaticamente ridiretto su l’authentication end-point dell’IdP. Compare una form che richiede username e password.

Il numero di tentativi è limitato e se superato blocca l'uso della password.

L’IdP riceve username e password digitati dall’utente. La password viene memorizzata nello user store (un server LDAP configurato per la gestione delle credenziali utente) come risultato del calcolo della funzione di hash SHA-512 con SALT. La stessa procedura viene avviata, utilizzando la username (opportunamente qualificata come DN (distiguished name) come chiave di accesso e l’impronta SHA-512 con SALT della password come meccanismo di verifica. Se i dati coincidono l’IdP rilascia la lista delle asserzioni SAML valide per l’utente.

## Meccanismi di autenticazione informatica a Livello 2 SPID (LoA3)

### Descrizione OTP via SMS

L’utente dopo aver inserito correttamente le proprie credenziali di Livello 1 SPID attiverà il seguente processo:

1. L’IdP provvede ad inviare un SMS al numero di telefono associato alle credenziali un codice numerico casuale di 8 cifre associato ad un prefisso alfanumerico di 3 caratteri (ad esempio: ATQ-98511560). Il numero di tentativi è limitato, se superato l'utente deve tornare al SP e richiedere una nuova autenticazione.
2. L’utente una volta ricevuto il messaggio contenente il codice, provvederà ad inserirlo in una form di login che presenterà tra l’altro il prefisso alfanumerico (ATQ- nell’esempio precedente). Questo meccanismo è necessario per prevenire attacchi men-in-the-middle perché il codice è noto solo all’IdP ed all’utente.
3. L’autenticatore ricevuto via HTTPS il codice numerico lo confronterà con quello generato per la sessione corrente dell’utente e se corretto procederà al rilascio delle asserzioni relative all’utente (SAML).

### Descrizione OTP via App

L’utente dopo aver selezionato il metodo di autenticazione basato su OTP, visualizzerà una form che richiede le credenziali di Livello 1 SPID ed un campo relativo alla OTP generata attraverso l’App avviando il seguente processo a carico del modulo di autenticazione dell’IdP:

L’IdP estrarrà il seed associato al profilo utente (mantenuto cifrato nello user store) e ricalcolerà l’OTP a partire dall’ora corrente. Qualora l’OTP calcolato e quello ricevuto non dovessero corrispondere, provvederà ad effettuare di nuovo il calcolo per 2 intervalli in avanti (ora corrente + 30 sec. ed ora corrente + 60 sec) e per due intervalli nel passato (ora corrente – 30 sec ed ora corrente – 60 sec.) se nessuna di queste corrisponderà l’autenticazione fallirà altrimenti saranno rilasciate le asserzioni SAML previste per l’utente.

L’IdP ricevuto via HTTPS il codice numerico lo confronterà con quello ha autonomamente generato per la sessione corrente dell’utente e se corrispondono procederà al rilascio delle asserzioni relative all’utente (SAML).

## Meccanismi di autenticazione informatica a Livello 3 SPID (LoA4)

L’IdP in questa fase per l’implementazione di un meccanismo di autenticazione di Livello SPID 3 utilizza l’implementazione built-in nel web server del protocollo TLS così come descritto dalla specifica RFC 5246 The Transport Layer Security (TLS) Versione 1.2. Attraverso tale protocollo è possibile, nella fase di negoziazione della chiave di sessione utilizzata per implementare un canale di trasporto sicuro con cifratura end-to-end, richiedere la mutua autenticazione dei due End-Point. In questo caso il protocollo prevede lo scambio dei certificati digitali (X.509) dei due End-Point per stabilire l’identità reciprocamente. Se il protocollo ha successo i dati del certificato dell’utente saranno disponibili ai livelli superiori (applicazioni). L’utente deve configurare la propria smart card (CNS) come uno store di certificati accessibile attraverso una interfaccia PKCS#11. E’ pertanto necessario che l’utente disponga della libreria PKCS#11 relativa alla coppia “tipo Smart Card” / “Tracciato dati CNS”. Questo store dovrà essere reso accessibile anche al browser perché possa presentare il certificato presente sulla smart card ogni volta che viene richiesta l’autenticazione per proseguire la navigazione.

Dopo che il server ha inviato il proprio certificato il protocollo prevede tra i vari passi:

* lo scambio dei certificati (utilizzando il messaggio CertificateRequest)
* la verifica del certificato (utilizzando il messaggio CertificateVerify) attraverso la firma di un messaggio negoziato in precedenza utilizzando la chiave privata relativa al certificato inviato. Il server dovrà verificare tale firma utilizzando la chiave pubblica disponibile nel certificato, dopo aver verificato preliminarmente la validità del certificato presso la Certification Authority che lo ha rilasciato.

L’IdP dopo aver configurato una risorsa (pagina web) che richiede la mutua autenticazione per l’accesso automaticamente, attiverà il protocollo TLS con mutua autenticazione dopo aver ridiretto l’utente verso la risorsa protetta.

Se il protocollo termina con successo, il modulo del web server che implementa il SecureTransportLayer renderà disponibili tutti i dati presenti sul certificato utilizzato dall’utente.