

Servizio di autenticazione SPID CIE eIDAS

Allegato Tecnico A

Sommario

[Premessa](#)

[Storia del documento](#)

[Definizione e Acronimi](#)

[Descrizione del Servizio](#)

[Aspetti tecnici](#)

[Descrizione del servizio offerto da Trentino Digitale](#)

[Attivazione dei servizi dell'Ente](#)

[Processo di attivazione dei servizi](#)

[Livelli di servizio per l'attivazione](#)

[Obblighi dell'Ente come aggregato](#)

[Esercizio del Servizio](#)

[Disponibilità del servizio](#)

[Assistenza in Esercizio](#)

[1. Help Desk](#)

[2. Gestione e manutenzione](#)

[Livelli di servizio](#)

[Trattamento dei dati personali](#)

Premessa

Il presente documento descrive in modo sintetico il servizio di autenticazione, fornito da Trentino Digitale S.p.A., per l'accesso ai servizi digitali della Pubblica Amministrazione del sistema trentino, nel rispetto delle normative vigenti.

Storia del documento

Versione	Data	Modifiche apportate
1.0	12.08.2024	Prima stesura

Definizione e Acronimi

Utente: cittadino (persona fisica) oppure impresa (persona giuridica) in possesso di una identità digitale, rilasciata da un Identity Provider (IdP), con la quale può richiedere l'accesso ai servizi digitali erogati da un Service Provider (SP).

Identità Digitale: rappresentazione informatica della corrispondenza biunivoca tra un utente e suoi dati identificativi, verificata attraverso l'insieme delle informazioni raccolte e registrate in forma digitale;

Identity Provider (IdP): soggetto abilitato a identificare gli utenti e a rilasciare e gestire le identità digitali, nel rispetto dei regolamenti e delle normative vigenti.

Service Provider (SP): soggetto che eroga un servizio digitale (online) agli utenti in possesso di una identità digitale rilasciata da un Identity Provider (IdP) a seguito della sua autenticazione informatica.

Federazione: insieme di soggetti che garantiscono la fiducia tra tutti i suoi componenti siano questi Identity Provider che Service Provider

Soggetto Aggregatore (SA): soggetto che fa da tramite verso IdP, consente la registrazione degli SP e semplifica l'operatività nella federazione.

Autenticazione Informatica: operazione di verifica della validità delle credenziali di accesso utilizzate dall'utente effettuata dal gestore dell'identità digitale (IdP), su richiesta del fornitore di servizi (SP), al fine di convalidarne l'identificazione informatica;

SPID: Sistema Pubblico di Identità Digitale, istituito ai sensi del Codice Amministrazione Digitale (CAD), che permette a cittadini ed imprese di accedere ai servizi online della Pubblica Amministrazione, e dei privati aderenti, utilizzando un'identità digitale unica.

CIE: Carta di Identità Elettronica è il documento d'identità dei cittadini italiani emesso dal Ministero dell'Interno e prodotto dal Poligrafico e Zecca dello Stato che permette ai cittadini l'accertamento dell'identità del possessore e può essere utilizzata per l'accesso ai servizi online delle Pubbliche Amministrazioni.

eIDAS: Regolamento UE n° 910/2014 (electronic IDentification Authentication and Signature) che fornisce la base normativa a livello europeo per i servizi fiduciari e i mezzi di identificazione elettronica negli stati membri.

CAD: Codice dell'Amministrazione Digitale, D. Lgs. 82 del 2005.

CNS: Carta Nazionale dei Servizi

CPS: Carta Provinciale dei Servizi, aderente al circuito delle Carte Nazionali dei Servizi

Descrizione del Servizio

Il servizio di autenticazione fornito da Trentino Digitale S.p.A. permette agli utenti in possesso di una identità digitale SPID, CIE, CPS, CNS, o identità digitali nazionali rilasciate da altri paesi europei, riconosciute in ambito eIDAS, di accedere ai servizi delle Pubbliche Amministrazioni della Provincia Autonoma di Trento, Soci di Trentino Digitale S.p.A, e altri Enti, principalmente del sistema trentino.

Trentino Digitale agisce come facilitatore offrendo agli Enti pubblici (soggetti aggregati) la possibilità di rendere accessibili i rispettivi servizi digitali tramite le identità digitali (SPID e altre riconosciute in ambito eIDAS) e gli strumenti CIE, CPS e CNS.

Tale azione si rende possibile grazie ad una infrastruttura tecnologica centralizzata¹ gestita da Trentino Digitale S.p.A., nel rispetto dei regolamenti e delle normative. Tale piattaforma garantisce agli Enti Soci e al sistema trentino l'assolvimento degli adempimenti normativi favorendo e semplificando al tempo stesso l'utilizzo dei servizi da parte dei cittadini.

Aspetti tecnici

L'infrastruttura tecnologica centralizzata di Trentino Digitale S.p.A., è un Gateway che permette ai Service Provider di identificare l'utente tramite protocollo OIDC e interagisce con la federazione tramite protocollo OIDCFederation o SAML a seconda del protocollo adottato dall'IDP. Per la verifica delle identità digitali i Service Provider collegati possono richiedere all'IdP scelto dall'utente (cittadino) l'autenticazione informatica.

Descrizione del servizio offerto da Trentino Digitale

Il servizio permette l'accesso alle identità digitali SPID, CIE, CPS, CNS e di EIDAS.

Ogni SP definisce il livello e il tipo di autenticazione e il set di attributi minimi necessari per l'operatività del servizio.

Trentino Digitale fornisce supporto agli Enti per la determinazione del livello di sicurezza per ciascun servizio coerentemente con le indicazioni nazionali. A tal fine, si ricorda che i livelli di sicurezza per l'autenticazione e l'accesso ai servizi sono tre: autenticazione a un fattore, ovvero password (SPID Livello1); autenticazione a due fattori (SPID Livello2); autenticazione basata su certificati digitali, ad esempio smart card (SPID Livello3).

Attivazione dei servizi dell'Ente

L'attivazione del servizio richiede la nomina di un proprio referente che sarà il soggetto titolato a richiedere, attraverso le modalità nel seguito descritte, l'attivazione dei servizi di autenticazione e verificarne il corretto funzionamento.

L'Ente si impegna a comunicare il proprio referente al momento dell'adesione al servizio e a comunicare tempestivamente eventuali variazioni.

¹ Infrastruttura tecnologica denominata "AdC" (Autenticazione del Cittadino) in corso di evoluzione su "AAC" (Authentication & Authorisation Control).

L'attivazione dei servizi di autenticazione richiede al service Provider, come prerequisito tecnologico, l'adozione del protocollo di autenticazione OpenID e la predisposizione dei propri sistemi secondo il modello tecnico organizzativo definito dalla Provincia Autonoma di Trento in delibera di G.P. nr. 1149 di data 26/07/2024. Si fa presente che l'evoluzione delle identità digitali, sia dal punto di vista tecnologico che tecnico-organizzativo, potrà richiedere ulteriori requisiti che saranno aggiornati e comunicati.

Trentino Digitale fornisce il supporto per l'integrazione mediante il nuovo protocollo OpenID.

Processo di attivazione dei servizi

Il processo di adesione è definito dalla Delibera di Giunta 1149 del 26/07/2024 a cui si rinvia per i dettagli. L'attivazione del servizio, da parte di Trentino Digitale, avviene attraverso la configurazione della piattaforma in ambiente di *pre-produzione* e prevede una fase di verifica da parte del referente dell'Ente che dovrà comunicare esplicitamente a Trentino Digitale il corretto funzionamento del servizio. Successivamente Trentino Digitale effettua la configurazione in ambiente di produzione con una ulteriore verifica da parte del referente dell'Ente che dovrà comunicare esplicitamente a Trentino Digitale il corretto funzionamento del servizio in produzione.

Si fa presente che rimane a carico di ciascun Ente la responsabilità delle soluzioni software che si intendono integrare con la porta di accesso della Provincia Autonoma di Trento: eventuali modifiche successive all'attivazione dovranno essere comunicate come descritto nel portale provinciale nella sezione Servizi "Utilizzo infrastruttura autenticazione provinciale e attivazione servizi online" url:

[Utilizzo infrastruttura autenticazione provinciale e attivazione servizi online / Servizi / Homepage - Provincia autonoma di Trento.](#)

Livelli di servizio per l'attivazione

Trentino Digitale S.p.A. garantisce i seguenti livelli di servizio (SLA) dal momento in cui si dispone di tutte le informazioni necessarie. I valori temporali indicati sono al netto del tempo necessario all'Ente per fornire ulteriori informazioni o chiarimenti su aspetti inizialmente non specificati e del tempo necessario per l'attivazione da parte della federazione.

Parametro	Valore	SLA (su base quadrimestrale)
Tempo di lavorazione di una richiesta di attivazione o modifica dell'Ente	10 giorni lavorativi	90% dei casi

Obblighi dell'Ente come aggregato

Si rinvia a quanto indicato nell'articolo 2 dell' "Accordo di collaborazione per favorire l'accesso ai servizi digitali tramite adesione all'infrastruttura di autenticazione provinciale"

allegato alla delibera 1149 del 26/07/2024 che dovrà essere sottoscritto tra l'ente e la Provincia Autonoma di Trento.

Esercizio del Servizio

Disponibilità del servizio

Il servizio è disponibile all'utenza in modalità 24x7 ad eccezione delle finestre temporali necessarie per eventuali manutenzioni e per cause non imputabili a Trentino Digitale e alla piattaforma AAC.

La disponibilità del servizio viene misurata sul perimetro del Data Center di Trentino Digitale.

Parametro	Livello di Servizio
Tempo di disponibilità annuo	99,98% al netto di fermi 99,96% comprendendo i fermi programmati

Trentino Digitale procede ad effettuare operazioni di manutenzione programmata, anche durante le ore di normale apertura degli uffici. Rientrano nelle attività di manutenzione programmata tutti gli aggiornamenti correttivi, funzionali e di sistema. Nel caso in cui la manutenzione programmata richieda l'indisponibilità del servizio, questa sarà preventivamente notificata per email ai referenti degli Enti. Nella comunicazione verranno forniti gli estremi temporali presunti del fermo, non vincolanti per Trentino Digitale.

In caso di un evento di manutenzione programmata Trentino Digitale si premurerà di darne opportuna comunicazione con un anticipo di almeno 72 ore rispetto al fermo dei servizi.

Parametro	Valore	SLA (su base quadrimestrale)
Tempo minimo di avviso in caso di disservizio per manutenzione programmata di competenza -di Trentino Digitale S.p.A.	3 giorni solari	90% dei casi

Assistenza in Esercizio

Trentino Digitale fornisce due tipi di assistenza in esercizio:

- Servizio di help desk
- Gestione e manutenzione

Considerato che il servizio Gateway AAC prevede l'integrazione con servizi degli Enti, si fa presente che rimane a carico di ciascun Ente la responsabilità dei servizi integrati, e da loro erogati, pertanto l'Ente deve effettuare la corretta diagnosi in caso di malfunzionamenti in modo da identificare con opportuno grado di precisione eventuali problemi ritenuti in capo al servizio AAC. La segnalazione di eventuali malfunzionamenti da parte del referente

dell'Ente, a seguito di un'accurata diagnosi nell'ambito del proprio dominio, sarà oggetto di analisi congiunta in modo da determinarne la natura e presa in carico da Trentino Digitale qualora dovuta al servizio di autenticazione AAC.

1. Help Desk

L'assistenza e la segnalazione di eventuali malfunzionamenti è garantita attraverso i canali opportunamente predisposti da Trentino Digitale per la Pubblica Amministrazione:

<https://www.trentinodigitale.it/Richieste/Servizio-assistenza-per-utenti-della-P.A>

2. Gestione e manutenzione

Trentino Digitale garantisce la gestione e manutenzione del servizio fornendo supporto agli Enti e ai cittadini e garantendone il funzionamento nel rispetto di livelli di servizio previsti. In particolare, si precisa che per manutenzione correttiva si intendono gli interventi di correzione di malfunzionamenti del sistema che non possono essere risolti attraverso semplici operazioni di configurazione, ma necessitano di operazioni di modifica software oppure aggiornamento di una o più componenti del sistema, purché inerenti funzionalità già previste dal sistema.

Livelli di servizio

I valori di SLA, su base quadrimestrale, riportati di seguito si riferiscono alla finestra temporale disponibilità del servizio di Help Desk ed esclusivamente alle attività di competenza di Trentino Digitale e relativamente al servizio di autenticazione AAC.

Parametro	Valore	SLA (su base quadrimestrale)
Tempo di presa in carico di un malfunzionamento dovuto al sistema AAC	60 minuti	90% dei casi
Tempo di diagnosi e risoluzione, anche provvisoria, di malfunzionamenti bloccanti che non richiedono manutenzione correttiva	240 minuti	85% dei casi
Tempo di diagnosi risoluzione, anche provvisoria, di malfunzionamenti non bloccanti che non richiedono manutenzione correttiva	480 minuti	85% dei casi

Per la risoluzione dei malfunzionamenti rimangono escluse cause non imputabili a Trentino Digitale e alla piattaforma di autenticazione AAC.

Trattamento dei dati personali

Le Infrastrutture Digitali di Trentino Digitali sono adeguate ai requisiti ACN per ospitare dati ordinari (AI1) e critici (AI2) e sono collocate a Trento.