ACADEMY

SPID & CIE

Relazione, scenari e catene di trust

Team per la Trasformazione Digitale, struttura di supporto al Commissario Straordinario dell'Attuazione dell'Agenda Digitale Luca Attias

Valerio Paolini
Technical Project Manager
valerio@teamdigitale.governo.it

Luca Bonuccelli
Technical Project Manager
luca.bonuccelli@teamdigitale.governo.it

Identità

Definizione Formale

Il complesso dei dati personali caratteristici e fondamentali che consentono l'individuazione o garantiscono l'autenticità, specialmente dal punto di vista anagrafico o burocratico.

Definizione Funzionale

L’insieme di tratti e caratteristiche che permettono di riconoscere in modo univoco una persona al fine di poter interagire con questa.

Chi sono? Cosa sono? Cosa posso fare?

Anagrafe

L'anagrafe è un registro della popolazione, tenuto dall'amministrazione di un qualunque ente (un comune, una regione, uno stato) ai fini di riportare i mutamenti demografici dovuti a cause naturali (come nascite, morti, migrazioni) e civili (per esempio, matrimoni e unioni civili).

Il Regno d'Italia istituì presso ogni Comune la prima anagrafe non obbligatoria con il Regio Decreto 2105/1864, resa poi obbligatoria con Regio Decreto 297/1871.

Se non sei in anagrafe non esisti!

Anagrafe & ANPR

ANPR corrisponde alla somma di tutti i registri ed abbatte i limiti causati dalla parcellizzazione: le amministrazioni potranno dialogare in maniera efficiente tra di loro, avendo una **fonte unica e certa** per i dati dei cittadini.

ANPR
Anagrafe Nazionale Popolazione Residente

Se sei in ANPR è tutto più semplice

L’origine della catena di trust

Iscrizione di un nuovo nato

- Genitori
- Ufficiale di Anagrafe
- Iscrizione a ANPR
- Attribuzione Codice Fiscale

Il primo anello della catena fiducia
è l’ufficiale di anagrafe

Uso della catena di trust

L'affidabilità di quanto registrato nell'anagrafe è base per poter certificare informazioni come:

- Esistenza di un soggetto
- Identità di un soggetto
- Stato civile
- Residenza

La catena di trust viene utilizzata per produrre prove

Rilascio della Carta d'Identità

Un esempio di prodotto della catena di trust è il rilascio della carta di identità.

La carta di identità può essere emessa solo da un ufficiale di anagrafe, che consulta la presenza in anagrafe del soggetto interessato e basa l'identificazione su un altro documento oppure su altre persone in grado di testimoniare l'effettiva identità del cittadino.

La carta di identità è la "mobilizzazione" della catena di fiducia iniziata con l'iscrizione in anagrafe.

La carta di identità è la mia prova anagrafica portatile

La Carta d'Identità Elettronica

Un supporto in policarbonato personalizzato mediante la tecnica del laser engraving con la foto e i dati del cittadino e corredato da elementi di sicurezza (ologrammi, sfondi di sicurezza, micro scritture, guilloches ecc.).

Contiene le mie informazioni anagrafiche.

Un microprocessore a radio frequenza che costituisce una componente elettronica di protezione dei dati anagrafici, della foto e delle impronte del titolare da contraffazione.

Contiene un certificato di autenticazione.

La CIE è sicura

Dove stanno le impronte digitali?

La rilevazione delle impronte digitali è prevista per ciascun cittadino di età maggiore o uguale a 12 anni.

Le impronte digitali (due) verranno scritte in sicurezza all'interno della propria CIE e **non conservate in nessun altro luogo.**

Per leggere le impronte è necessaria un'autorizzazione e una chiave fornite dal Ministero dell'Interno.

Utilizzi del Documento d'Identità

- identificazione fisica
- documento di viaggio
- identificazione elettronica
  - In scenario a bassa sicurezza
  - in scenario ad alta sicurezza
- Codice Fiscale

Identificazione Fisica

- In banca
- In un ufficio
- Per stipulare un contratto
- Per strada
- In un albergo
- All’aeroporto

Per dimostrare che “io sono davvero io”

Validazione

La validazione può avvenire controllando le caratteristiche fisiche della carta oppure utilizzando gli strumenti elettronici.

IPZS ha sviluppato l'app IDEA che consente di validare un documento.

Con IDEA dunque il possessore di un documento elettronico (carta d'identità elettronica, passaporto elettronico, permesso di soggiorno elettronico) può verificarne l'autenticità e appurare che i dati memorizzati nel chip corrispondano a quanto stampato sul documento.

Identificazione elettronica a bassa sicurezza

Numero Identificativo Servizi, **NIS**, presente all'interno del microprocessore, leggibile senza alcuna condizione di accesso e garantito dalla firma digitale del Ministero dell'Interno.

Non è un dato parlante, ovvero dal numero non si può risalire direttamente ai dati del titolare: pertanto la lettura di questo numero non offre alcuna informazione sulla carta o sul titolare.

Dalla lettura di tale numero per i servizi autorizzati è possibile tuttavia risalire al codice fiscale del titolare della carta, interrogando un opportuno servizio messo a disposizione dal Ministero dell'Interno.

Scenari di Utilizzo

- Tornelli
- Marcatempo
- Trasporto pubblico locale
- Carte fedeltà

Identificazione Online

L'autenticazione online si basa su un certificato di autenticazione a bordo della CIE.
Il certificato contiene:

C	= IT
SN	= ROSSI
G	= BRUNA
SERIALNUMBER	= IDCIT-CA12345AA
CN	= RSSBRN80E56H501Y/123456789012

Per utilizzare il certificato è necessario conoscere il PIN (secondo fattore).

Autenticazione TLS

Lo schema di autenticazione prevede che il server ove è esposto il servizio online:

- conosca la Certification Authority
- controlli le liste di revoca

Inoltre l'utente "percepisce" solo il fornitore di servizi come controparte a cui eventualmente chiedere supporto.

Criticità: configurazione da ripetere per tutti i servizi, help desk, aggiornamenti, privacy; una volta inserito il pin, il certificato è utilizzato fino alla chiusura del browser senza che l'utente possa intervenire.

Modello CieID

L'autenticazione TLS avviene esclusivamente con il servizio

https://idserver.servizicie.interno.gov.it/

il quale produce una asserzione di autenticazione che viene inoltrata al Service Provider (esattamente come in SPID):

- Un unico punto di autenticazione
- Un unico punto di contatto/helpdesk
- Una unica UX
- Una unica implementazione per gli SP

Privacy

Stesso modello di privacy previsto per SPID:

il Ministero dell'Interno conosce solo l'ente presso cui si è effettuata l'autenticazione ma non il servizio che viene fruito.

“Firma con CIE”

Secondo l’articolo 61 del DPCM 22 febbraio 2013:

> L’utilizzo della Carta d’Identità Elettronica sostituisce, nei confronti della pubblica amministrazione, la firma elettronica avanzata ai sensi delle presenti regole tecniche per i servizi e le attività di cui agli articoli 64 e 65 del Codice dell’Amministrazione digitale.
>
> I formati sono i medesimi previsti per la firma qualificata.

Notifica ai sensi del Regolamento eIDAS

Affinché la CIE possa essere utilizzata come strumento di identificazione nei servizi online dei paesi membri dell'Unione Europa è necessario notificare alla Commissione Europea lo schema di identificazione basato su di essa.

Un'apposita commissione effettua la *peer review* per valutare gli aspetti di sicurezza e di aderenza al Regolamento eIDAS.

La notifica è attualmente in corso e dovrebbe concludersi entro la fine della primavera.

La catena di fiducia oltrepassa la frontiera Digital Single Market!

Emissione all'Estero

Progetto pilota di emissione entro la fine dell'estate presso:

- Ambasciata di Nizza
- Ambasciata di Vienna
- Consolato Generale di Atene

A regime presso tutti i paesi membri dell'Unione Europea.

SPID

SPID, il Sistema Pubblico di Identità Digitale, è la soluzione che ti permette di accedere a tutti i servizi online della Pubblica Amministrazione e dei privati aderenti con un'unica Identità Digitale utilizzabile da computer, tablet e smartphone.

spid
Sistema Pubblico di Identità Digitale

È una federazione di soggetti pubblici e privati che implementano il Sistema Pubblico di Identità Digitale composta da:

- Gestori di Identità
- Fornitori di Servizi
- Gestori di Attributi Qualificati

Lo Stato regolamenta e vigila.

Un'unica Identità Digitale

Rilascio Identità SPID

La catena di fiducia si può arricchire di un ulteriore anello:

dall'identità garantita dalla CIE si può ottenere una identità Digitale SPID

Per ottenere una identità SPID occorre:

- un documento di riconoscimento valido
- un indirizzo e-mail
- il numero di telefono del cellulare che usi normalmente
- tessera sanitaria con il codice fiscale (solo codice fiscale per l'estero)

SPID è un anello della catena di trust

Importanza del Processo di Riconoscimento

Il mondo digitale non è separato da quello reale.

- L'identità digitale se usata per accedere a servizi (esempio comprare una macchina, accedere a dati sensibili, firmare un contratto) deve avere le stesse garanzie di quella del mondo fisico.
- Il riconoscimento da parte del fornitore di identità è il passaggio fondamentale per creare una identità digitale da una fisica.

Questo il motivo della particolare attenzione nella fase di riconoscimento per ottenere una identità digitale (esempio: controllo in back office dei documenti di identità).

Identità digitale non è l'avatar dei Social Network

Utilizzo di SPID

SPID è utilizzabile per identificare il soggetto che accede ad un servizio on line erogato da un Ente Pubblico o da un Soggetto Privato.

Tutti i servizi on line erogati da Pubblica Amministrazione, dai gestori di servizi pubblici e dalle società a controllo pubblico, che necessitano di identificazione devono essere integrati in SPID.

Nel CAD ad esempio questi servizi devono offrire autenticazione con SPID:

- Elezione domicilio digitale
- Pagamenti
- Punto unico di accesso
- Sottoscrizione / firma con spid
- Consultazione del fascicolo informatico del procedimento

Privacy

L'IdP non conosce il servizio a cui l'utente accede.

L'SP richiede solo i dati di cui ha oggettivamente bisogno.

L'utente ha visione di cosa venga trasmesso dall'IdP all'SP.

L'utente può verificare quando è stata utilizzata l'identità.

La struttura operativa che eroga servizi non può coincidere con quella di un IdP.

La profilazione dell'utente è impedita da regolamento.

Livelli di Autenticazione

SPID prevede 3 livelli di autenticazione, con garanzie progressivamente maggiori.

Il primo livello permette di accedere ai servizi online attraverso un nome utente e una password scelti dall'utente (singolo fattore).

Il secondo livello permette l'accesso attraverso un nome utente e una password scelti dall'utente, più il possesso di un dispositivo (due fattori).

Il terzo livello, oltre al nome utente e la password ed il possesso di un dispositivo, prevede l'uso di crittografia asimmetrica (due fattori, il secondo basato su PKI)

Uso dei Livelli di Autenticazione

I servizi necessitano di un livello minimo di sicurezza nell'autenticazione in funzione del danno potenziale in caso di furto d'identità.

Danno potenziale per:

- il soggetto titolare dell'identità
- per il service provider
- per la società

Il livello minimo di sicurezza è scelto dal Service Provider

Attribute Authority

L’identità di SPID prevede di fornire ai servizi on line che ne abbiamo esigenza anche tratti qualificanti dell’utente (ordine professionale, qualifica, altro).

Le informazioni che costituiscono le asserzioni di attributo sono prelevate dinamicamente dalla fonte autorevole arricchendo l’identità.

Il Service provider non è più obbligato a richiedere autocertificazioni (che devono poi essere verificate).

L’autocertificazione non sarà più necessaria

“Firma con SPID”

SPID può essere usato anche per l’identificazione utile alla riconducibilità all’autore di documenti elettronici.

In particolare l’emananda linea guida prevista dall’articolo art 20 del CAD trova in SPID una base per la soluzione tecnologica.

Si potrà *firmare* con SPID

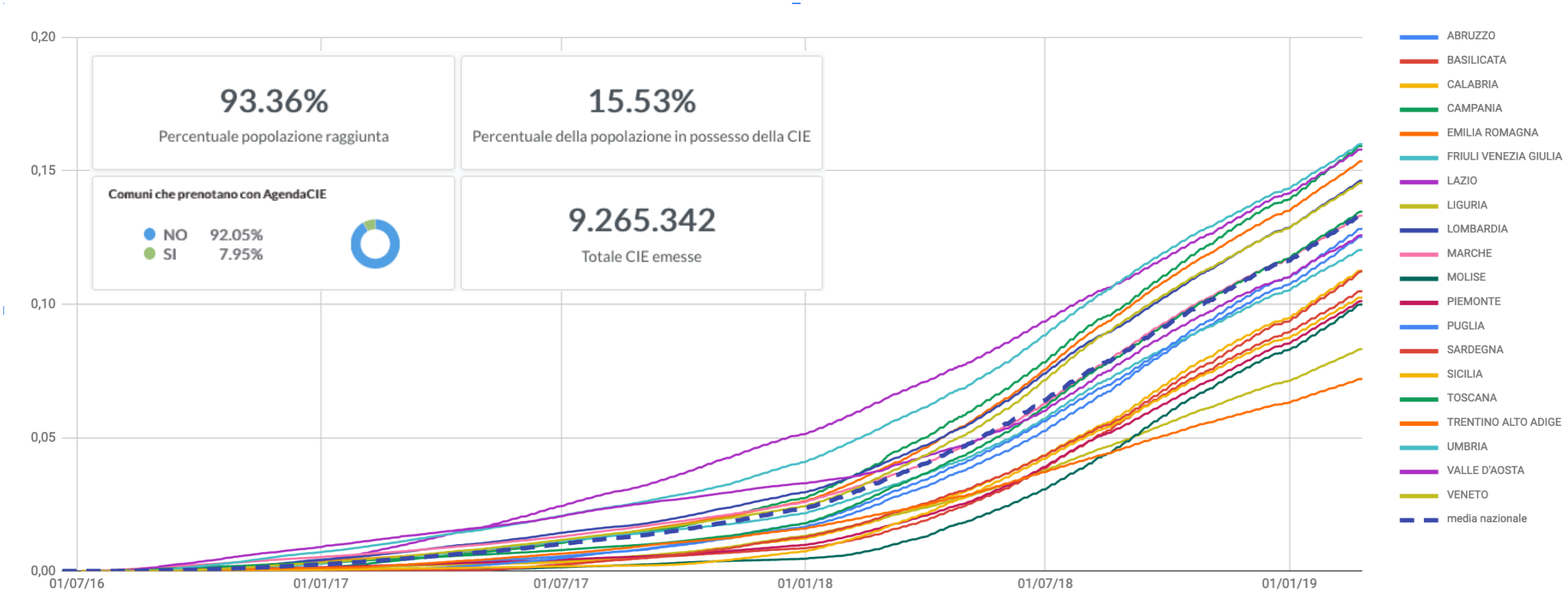
Notifica ai sensi del Regolamento eIDAS

La notifica è stata completata e pubblicata in gazzetta ufficiale EU il 10 settembre 2018

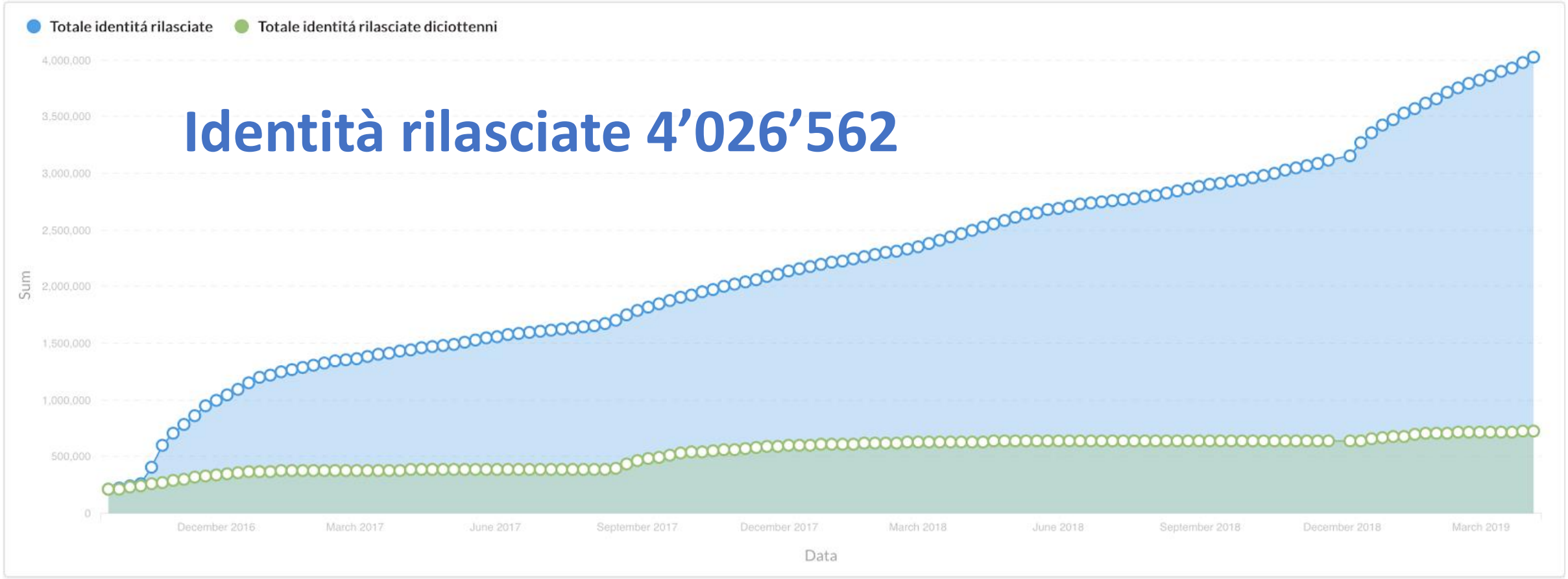
A decorrere dal 10 settembre 2019 SPID potrà essere utilizzato per fruire dei servizi on line di tutti gli stati membri UE

Digital Single Market!

CIE – i Numeri


93.36%
Percentuale popolazione raggiunta
15.53%
Percentuale della popolazione in possesso della CIE
Comuni che prenotano con AgendaCIE
NO 92.05%
SI 7.95%
9.265.342
Totale CIE emesse
0,20
0,15
0,10
0,05
0,00
01/07/16
01/01/17
01/07/17
01/01/18
01/07/18
01/01/19
ABRUZZO
BASILICATA
CALABRIA
CAMPANIA
EMILIA ROMAGNA
FRIULI VENEZIA GIULIA
LAZIO
LIGURIA
LOMBARDIA
MARCHE
MOLISE
PIEMONTE
PUGLIA
SARDEGNA
SICILIA
TOSCANA
TRENTINO ALTO ADIGE
UMBRIA
VALLE D'AOSTA
VENETO
media nazionale

SPID – i Numeri



CIE vs. SPID

- Identificazione on line
  - diversità biologica
  - gradazione del livello di autenticazione
  - SPID utilizzabile senza accessori HW (almeno fino a livello 2)
- CIE utilizzabile elettronicamente anche nel mondo fisico (NIS, MRTD)
- Con CIE si può ottenere SPID, con SPID non si può ottenere CIE
- Firma
  - CIE (FEA art. 61 DPCM 23 febbraio 2013, solo verso PPAA)
  - SPID (art. 20 CAD, universale)
- Attributi qualificati
  - SPID nativamente presenti
  - CIE attualmente solo attraverso modello di interoperabilità
- UE Digital Single Market → entrambi

Piano Triennale: Azioni SPID

Giugno 2019

Linee guida per il rilascio delle identità digitali per uso professionale
Linee guida user experience
Linee guida per l'implementazione di sistemi per la firma ex articolo 20 del Codice dell'amministrazione digitale attraverso SPID
Linee guida per l'adesione in SPID delle Attribute authority in qualità di gestori di attributi qualificati
Linee guida OpenID Connect

Ottobre 2019

è abilitato all'uso per l'accesso ai servizi online delle PA all'interno dell'Unione Europea

Dicembre 2019

Messa in esercizio del nodo FICEP.

Piano Triennale: Azioni CIE

Aprile 2019

Emissione della CIE all'estero nei consolati pilota

Avvio notifica eIDAS

Dicembre 2019

Integrazione della CIE come strumento di identificazione nei servizi online della PA.

Onboarding già operativo

Academy AD.28 "Carta di Identità Elettronica: scenari di integrazione nei servizi online"

https://www.cartaidentita.interno.gov.it/CIE3.0-ManualeSP.pdf

Scenario

Permesso per entrare nella ZTL

- mi collego al servizio del mio Comune
- mi identifico utilizzando SPID
- il servizio del Comune recupera i dati necessari dalle Attribute Authority:
  - la residenza da ANPR
  - i veicoli da me posseduti presso la MTR
- il servizio mi chiede di sottoscrivere le condizioni del servizio con Firma con SPID
- il permesso è erogato e salvato in un'apposita Attribute Authority che potrà essere utilizzata per esempio dai Vigili Urbani

Il permesso di accesso a zone limitate potrebbe essere consentito anche tramite la CIE, lette da apposite colonnine all'ingresso delle zone a traffico limitato.

Grazie per l'attenzione!

Domande?

Webografia

Team Trasformazione Digitale

https://teamdigitale.governo.it

SPID

https://www.spid.gov.it/
https://developers.italia.it/it/spid/
https://teamdigitale.governo.it/it/projects/identita-digitale.htm

CIE

https://www.cartaidentita.interno.gov.it/
https://developers.italia.it/it/cie/
https://teamdigitale.governo.it/it/projects/cie.htm