Anagrafe Nazionale della Popolazione Residente
e
Identità Digitale
fondamento della e-strategy per i cittadini

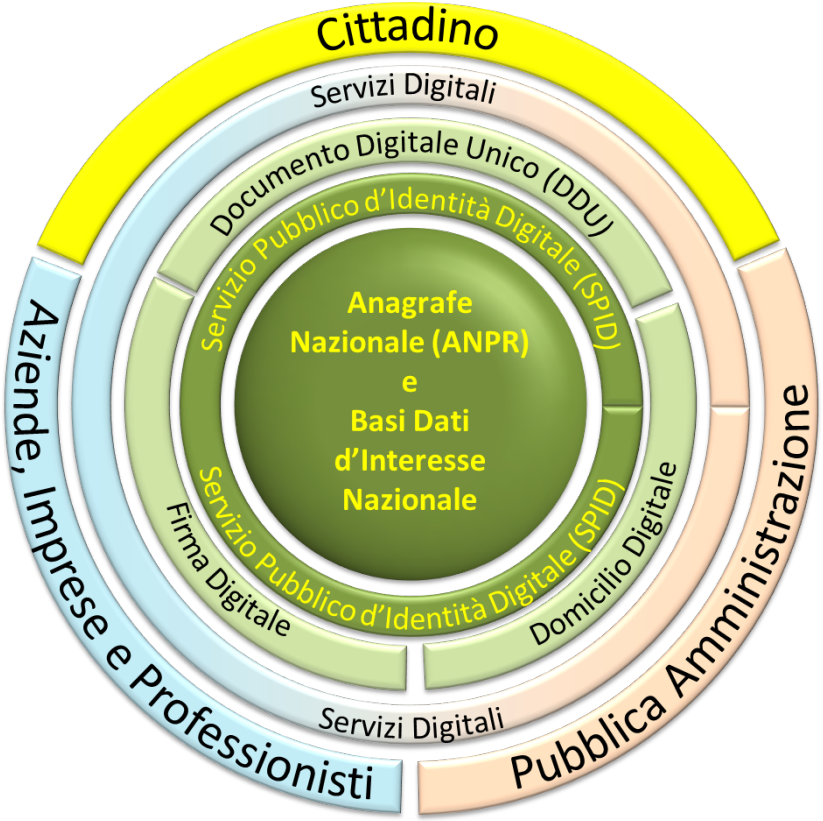
FORUM PA 2014

Relatore: Ing. Stefano Sappino

e-strategy per i cittadini

- Per innovare i rapporti tra pubblica amminstrazione e cittadini e migliorare l'efficienza interna della pubblica amministrazione occorre agire all'interno di un quadro organico e integrato di interventi che abilitino un effetto moltiplicativo dei singoli benefici

- Un insieme identificato di iniziative strettamente collegate sono:
  - Anagrafe Nazionale della Popolazione Residente
  - Identità Digitale
  - Domicilio Digitale
  - Firma Digitale
  - Documento Digitale



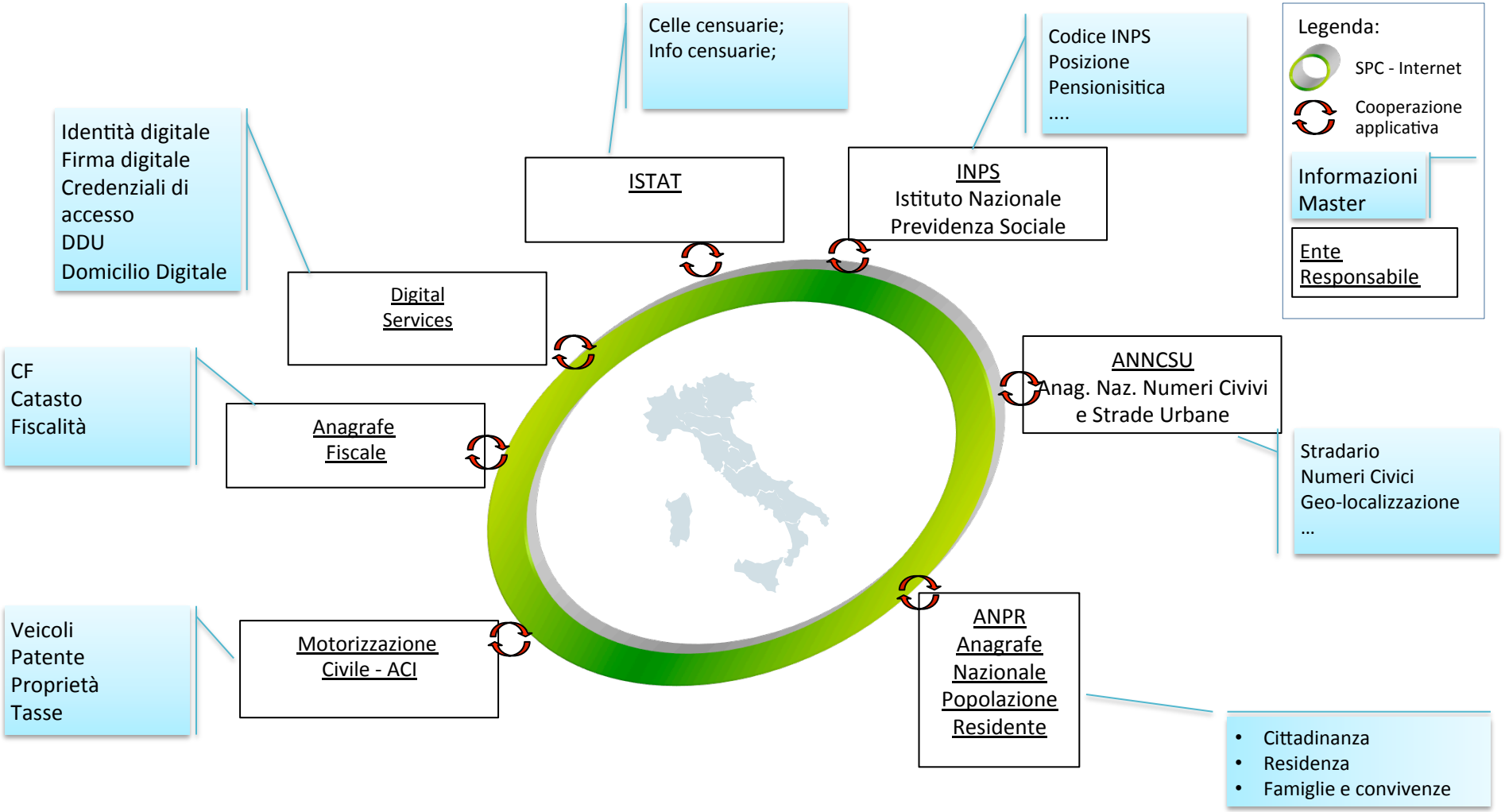
ANAGRAFE NAZIONALE DELLA POPOLAZIONE RESIDENTE (ANPR)

Anagrafe Nazionale della Popolazione Residente
Obiettivi e Benefici

- Anagrafe nazionale unica per il cittadini italiani ovunque residenti e stranieri residenti in Italia
- Aggiornamento in tempo reale e completa circolarità delle informazioni
- Fondamento della semplificazioni delle relazioni tra cittadini e PA, e tra PA (locali e centrali)
- Riduzione degli scambi informativi e innalzamento della qualità, con conseguente risparmio denaro e tempo per PA e Cittadini
- Hub di distribuzione di informazioni affidabili e aggiornate
- Cornerstone del sistema integrato di Basi Dati di Interesse Nazionale

Circolarità delle informazioni
Modello di cooperazione

CONCETTUALE



Anagrafe Nazionale della Popolazione Residente
Il percorso

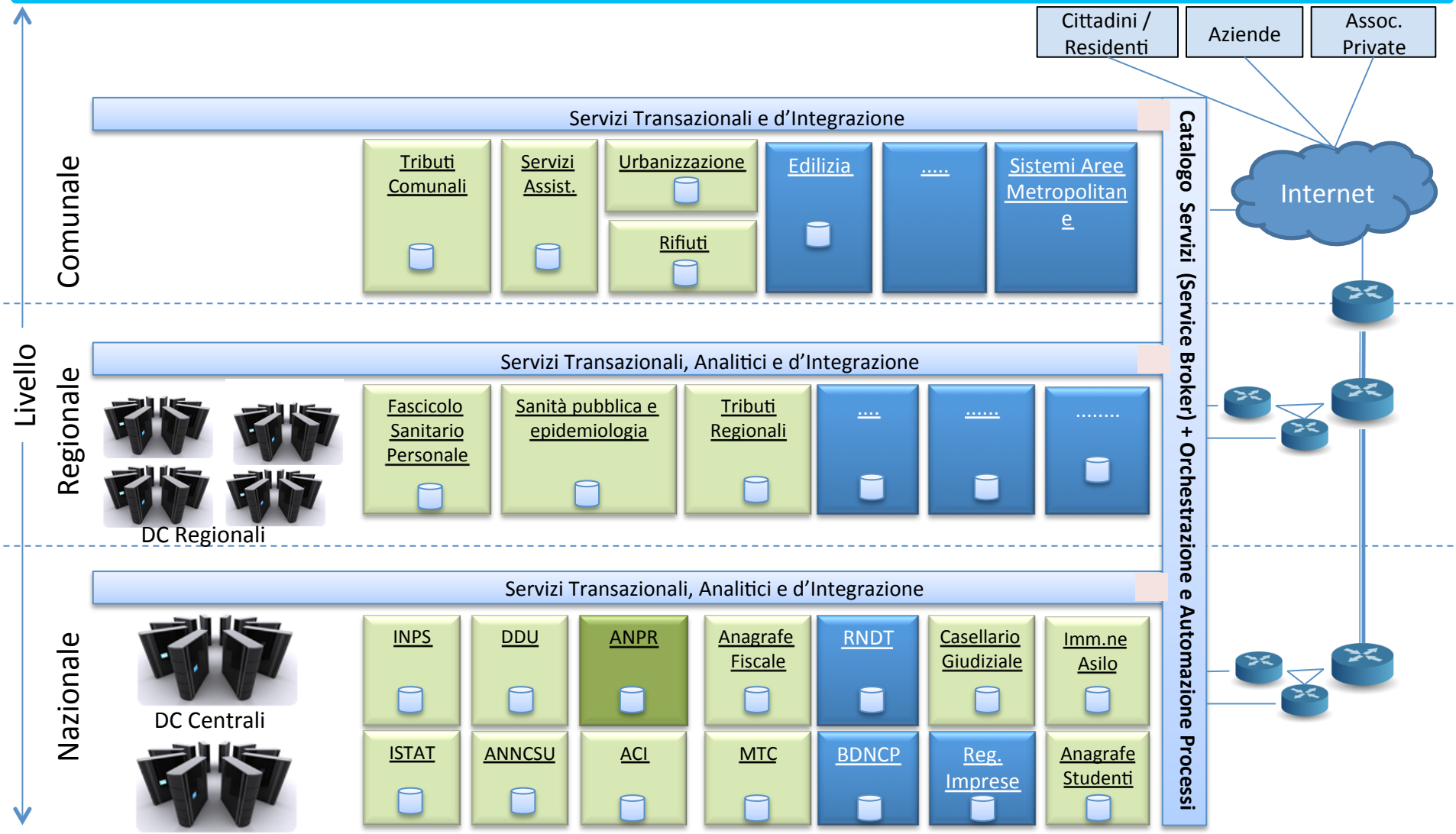
- Decreto di Istituzione ANPR: Decreto n° 109/2013 del Presidente del Consiglio dei Ministri
- Il programma attuativo è in sviluppo grazie alla stretta collaborazione di numerose istituzioni:
  - Ministeri dell'Interno e Ministero della Funzione Pubblica (proponenti)
  - Ministero degli Esteri
  - Ministero Economia e Finanza
  - Autorità garante per la protezione dei dati personali
  - ISTAT
  - ANCI
  - CISIS
  - Agid
  - SOGEI
- Gli enti coinvolti si coordinano attraverso un processo di program management condiviso

Anagrafe Nazionale della Popolazione Residente
Vantaggi

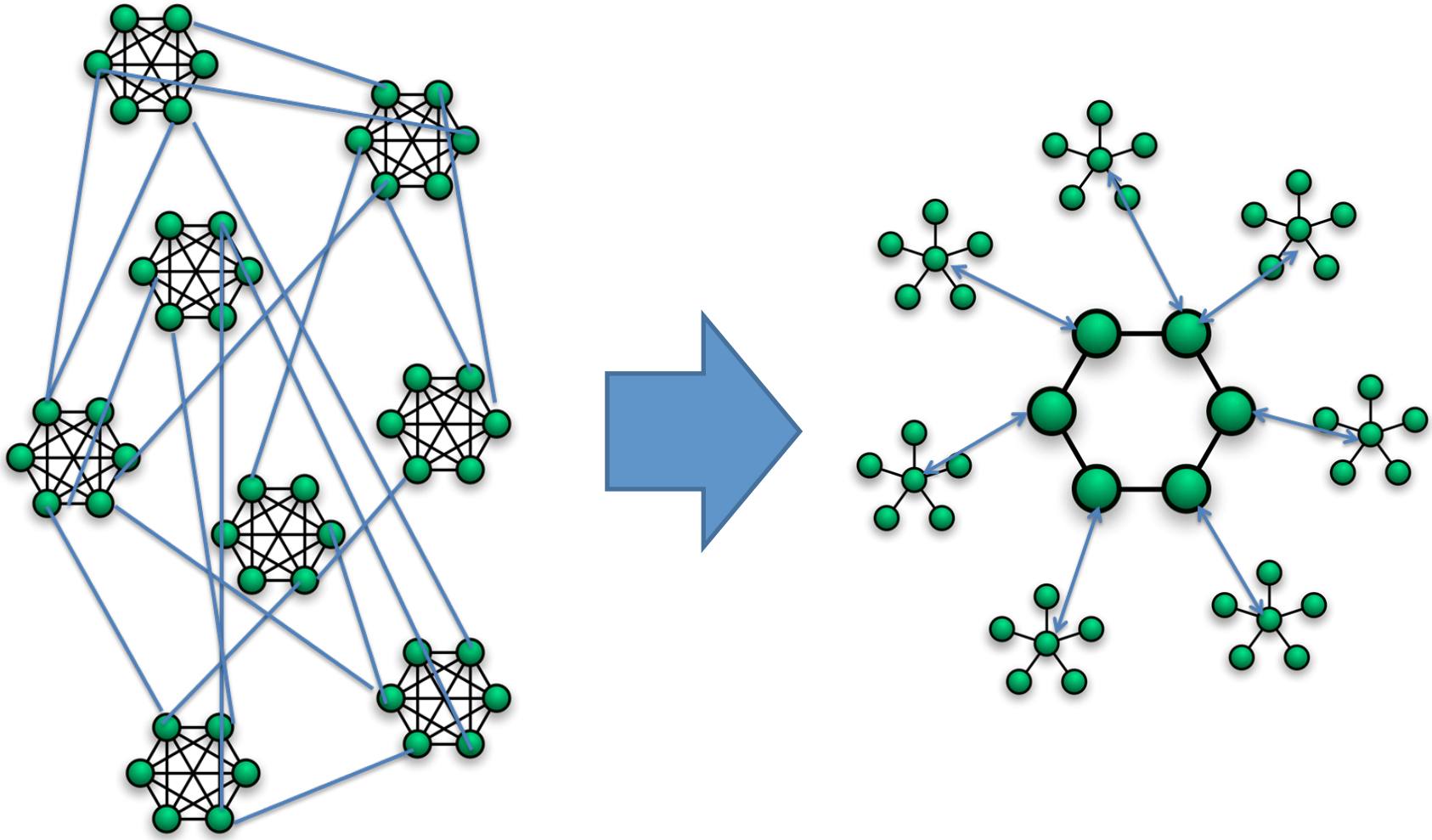
- Immediata disponibilità **Servizio Emissione Certificati Integrato** su Base Nazionale
- **Miglioramento** per cittadini e comuni delle **procedure "inter- comunali"**
- **Semplificazione** degli **adempimenti** comunali per l'**invio** delle informazioni **alle PA centrali**
- **Base per l'avvio** di significative **velocizzazioni e semplificazioni** delle **procedure** per il **funzionamento** dello **Stato**:
  - Dichiarazioni di nascita e morte (raccolta informazioni cause di morte);
  - Anagrafica degli assistiti;
  - Adempimenti relativi agli uffici di stato civile (integrazione del registro degli atti civili)
  - Censimento Permanente
  - ANNCSU - Archivio Nazionale dei Numeri Civici e delle Strade Urbane

Servizi e loro collocazione
Modello di Riferimento

CONCETTUALE



Efficienza della struttura informativa
Minori costi di gestione e migliorato funzionamento



SERVIZIO PUBBLICO D'IDENTITÀ DIGITALE (SPID)

Cos'è un'Identità Digitale?

Identificativo: 190023AA
IDProvider: ITABANK1

Attributi Identificativi Obbligatori:
Nome: Mario
Cognome: Rossi
Comune di Nascita: San Giuliano Terme
Sesso: M
Codice Fiscale: RSS MRA 85T10 A562S

Attributi non Identificativi Obbligatori:
email: mario.rossi@rossispa.it
Tipologia email: PEC
Indirizzo: via Ticino 1 – Milano

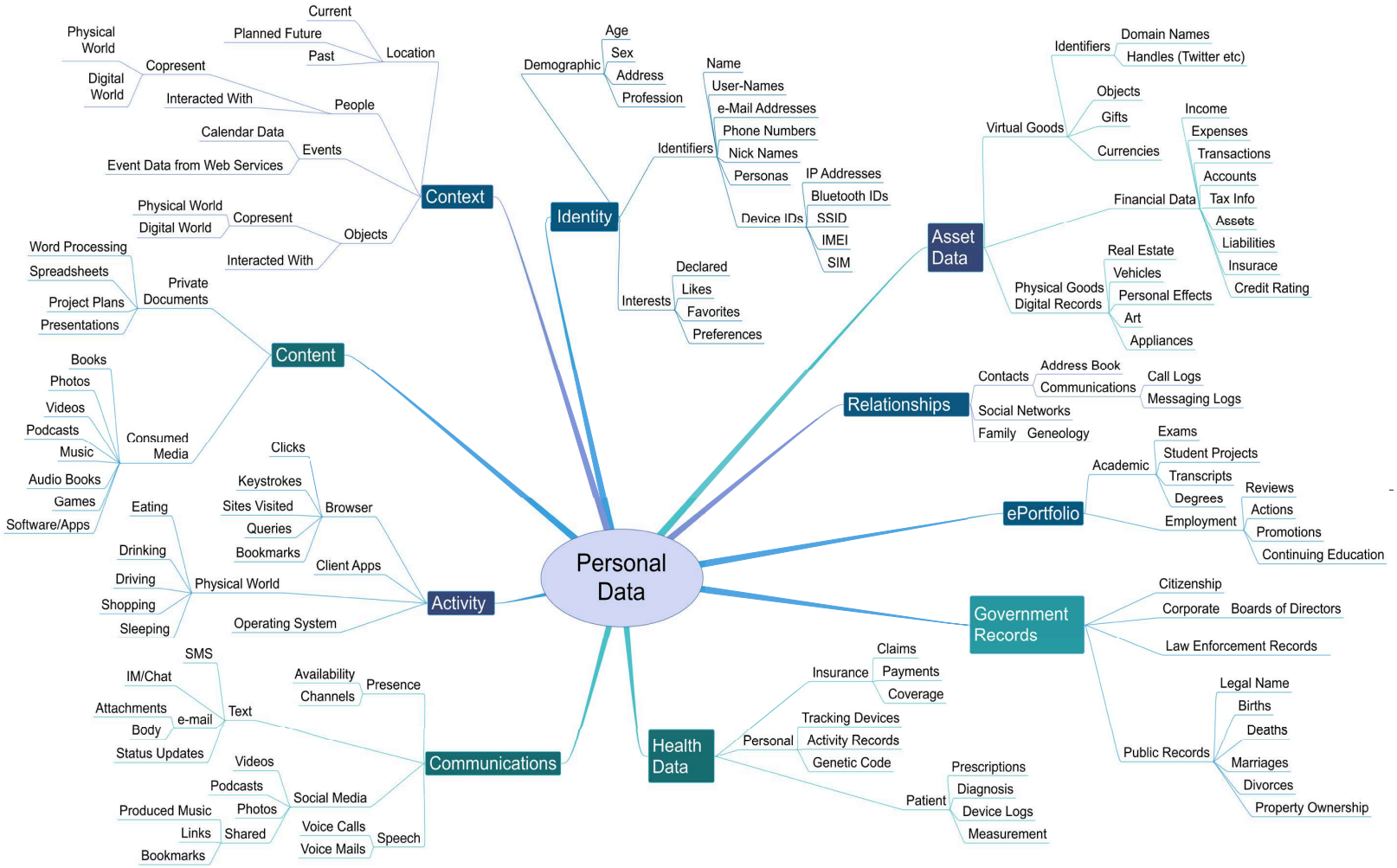
Attributi non Obbligatori:
Attributo 1…. Attributo N

Attributi Esterni - (esempi):
Firma Digitale
Casella PEC
Qualifica Professionale
Ruolo Societario

Credenziali:
Credenziale 1
Credenziale 2
…
Credenziale N

- L'Identità Digitale è l'insieme degli attributi, così come raccolti e registrati in forma digitale finalizzati all'accesso e alla fruizione di servizi erogati in rete
- E' Costituita da:
  - Identificativo univoco
  - Codice Fiscale
  - Attributi Identificativi Obbligatori (Nome, Cognome, Luogo di Nascita, Sesso, Codice Fiscale)
  - Attributi non Identificativi Obbligatori (Email, tipo email e indirizzo)
  - Eventuali attributi non obbligatori
  - Credenziali
- Inoltre, ulteriori Attributi esterni sono forniti dai Gestori di Attributi Qualificati

Identità Digitale parte integrante dell'ecosistema dei Dati Personali in evoluzione

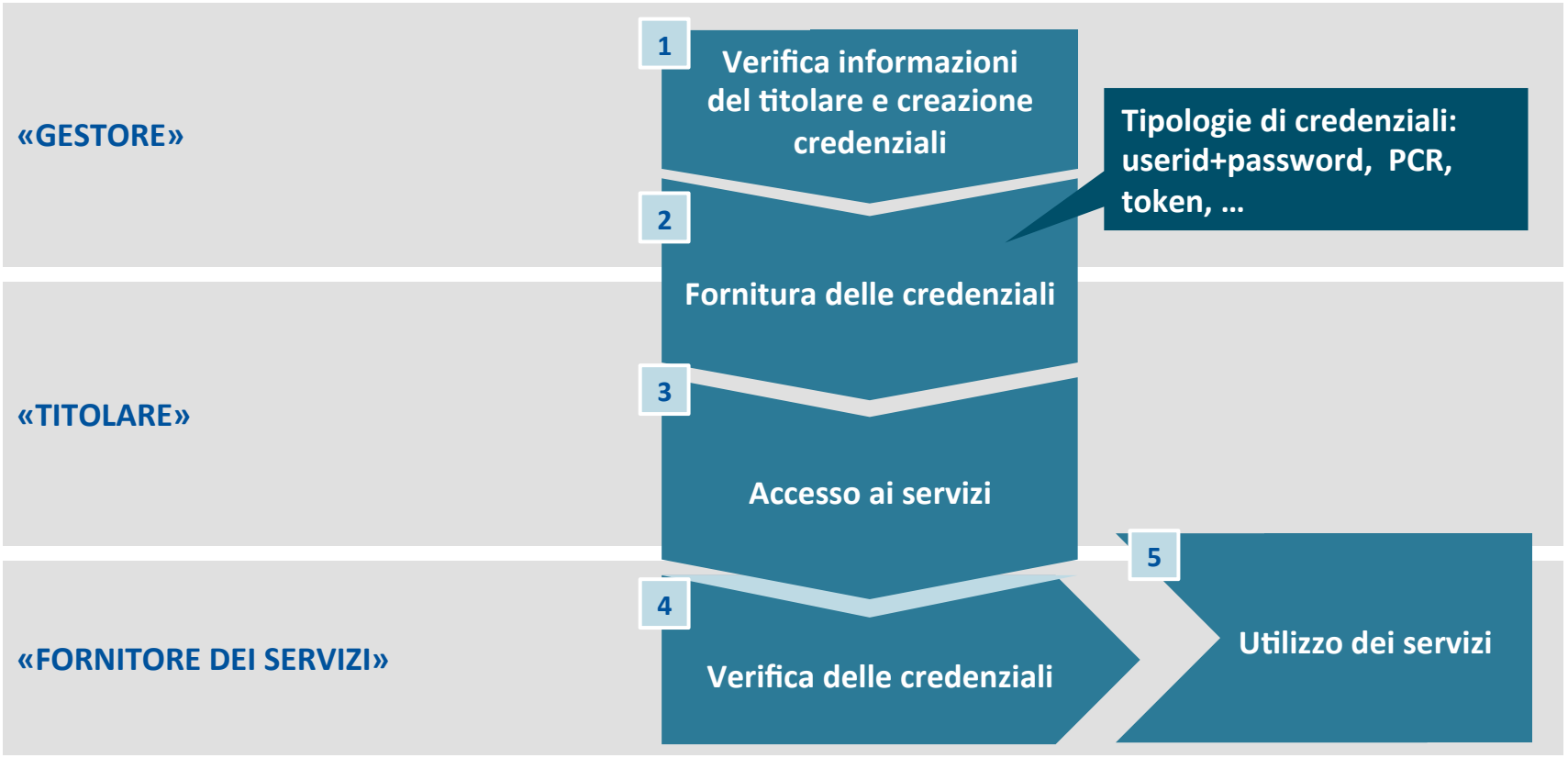


Fonte: World Economic Forum

Identità Digitale
Il ciclo di vita

Il ciclo di vita della gestione dell'identità digitale coinvolge tre soggetti:

- **Il «Titolare»**, per il quale l'identità è "creata"
- **Il «Gestore»,** che "crea" un'identità
- **Il «Fornitore dei servizi»**, che sulla base delle caratteristiche (attributi) dell'identità valuta quali servizi possono essere accessibili al Titolare dell'identità



Gli attori coinvolti

Titolare dell'Identità Digitale: è la persona che accede ai servizi digitali erogati da un Fornitore di Servizi, tramite una Identità Digitale

Gestore dell'Identità Digitale (Identity Provider): la persona giuridica che crea, rende disponibili e gestisce gli attributi utilizzati dall'utente al fine di dimostrare la propria Identità digitale;

Gestore di attributi qualificati: enti aventi per legge l'obbligo di certificare il possesso e la validità di attributi qualificati, abilitazioni professionali, poteri di rappresentanza o altri attributi.

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

Agenzia per l'Italia Digitale: emette il Regolamento Attuativo, accredita i Gestori dell'identità Digitale e i Gestori di Attributi Qualificati, pubblica il registro e vigila sulle attività degli operatori.

Fornitore di Servizi: è il soggetto privato o la pubblica amministrazione che eroga servizi via Internet per cui è richiesta una identificazione e autenticazione degli utenti

Modalità di rilascio di una identità Digitale

- Il Cittadino si rivolge ad un Identity Provider per il rilascio di una Identità Digitale
- L'Identity Provider, per mezzo di un proprio funzionario addetto, verifica l'Identità del Richiedente e crea l'Identità Digitale certificando la correttezza degli attributi Identificativi obbligaori
- Viene creato il primo set di credenziali, che vengono consegnate direttamente e in modo sicuro al Titolare.

- *Nel caso in cui il richiedente sia già in possesso di un documento elettronico (es. CIE, CNS, Carta di Firma), il rilascio di una identità Digitale potrà avvenire direttamente online e la credenziale del documento elettronico sarà abilitata come credenziale SPID. Il rilascio online potrà avvenire anche nel caso in cui il titolare sia già in possesso di una Identità SPID valida.*

I livelli di Sicurezza

- A differenza di altri progetti Europei, SPID prevede un unico livello di verifica secondo i requisiti più alti (verifica de visu).
- SPID prevede 3 livelli di sicurezza associati alla robustezza del sistema di credenziali per l'autenticazione, corrispondenti ai Livelli 2, 3 e 4 dello Standard ISO/IEC DIS 29115

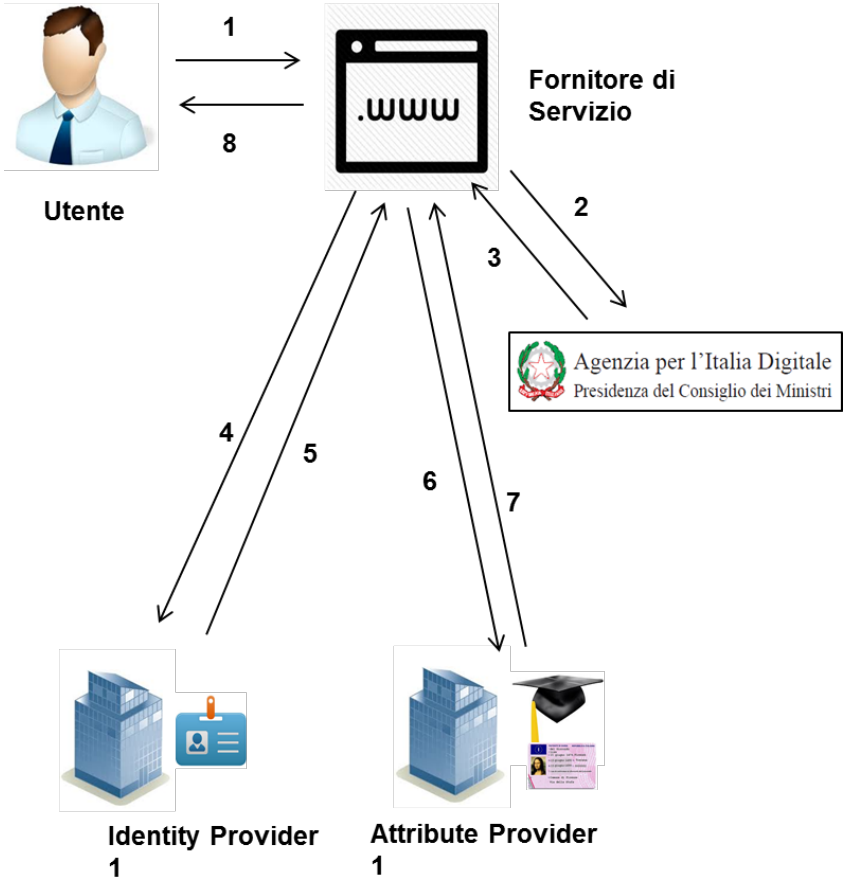
  - **Livello 2:** Sistemi di autenticazione ad 1 fattore (ad esempio Password)

  - **Livello 3:** Sistemi di autenticazione «Forte» a 2 fattori (ad esempio One Time Password)

  - **Livello 4:** Sistemi di autenticazione «Forte» a 2 fattori con l'obbligo di utilizzo di dispositivi hardware anti compromissione per la creazione e la conservazione delle chiavi segrete (ad esempio Smart Card o analoghi)

- Nella pubblica amministrazione sono consentiti esclusivamente i Livelli 3 e 4

Il funzionamento



Le interazioni Fondamentali

1. L'Utente richiede l'accesso ad un Servizio, fornendo il proprio identificativo e presentando una credenziale valida
2. Il fornitore di Servizio interroga il registro degli Identity Provider e Attribute Provider presso AgID
3. AgID restituisce copia del registro
4. Il Fornitore di servizio inoltra la richiesta di autenticazione all'Identity Provider corretto
5. L'identity provider, nel caso in cui l'utente disponga del corretto livello di credenziale, ne verifica la corrispondenza, fornendo al fornitore di servizio l'asserzione di identità e gli eventuali attributi richiesti.
6. (opzionale) Il Fornitore di servizio invia la richiesta di attributi all'Attribute Provider
7. (opzionale) L'Attribute Provider fornisce al fornitore di servizio gli attributi richiesti
8. L'utente autenticato viene autorizzato ad accedere al servizio o alla funzione richiesta

Benefici

- L'Istituzione di un Sistema Pubblico di Identità consentirà di disporre di Identità Digitali "sicure" (Trusted Identities)
- La diffusione di Identità Digitali sicure porterà una serie di benefici ai cittadini e agli erogatori di servizi pubblici e privati:
  - Semplificare per il cittadino l'accesso ai servizi della pubblica amministrazione
  - Creare un ecosistema digitale sicuro e "trusted" per cittadini e fornitori di servizi
  - Contrastare I fenomeni di crimine informatico e in particolare di furto d'identità
  - Elemento fondante per lo sviluppo dell'economia digitale del paese

Ecosistema digitale

- Per i cittadini, le imprese e le PA:
  - Maggiore efficienza e minori costi in termini tempo, spostamenti, adempimenti dovuti all'invio o alla verifica delle informazioni
  - Semplicità standard e condivisa
- Per i gestori di servizi:
  - La possibilità di rendere disponibili servizi avanzati e complessi possibili solo all'interno di un sistema "trusted" di utilizzatori e imprese
- Per lo sviluppo economico:
  - Diminuzione radicale delle ridondanze e delle inefficienze informative e dei costi che, in cascata, producono informazioni duplicate, non aggiornate, incerte, incomplete od errate di imprese e cittadini.
  - Forte spinta verso un funzionamento "in tempo reale" dei servizi
  - Apertura a nuove opportunità di sviluppo di servizi

BACKUP

L'Identità Digitale pone di fronte a nuove sfide

Fonte: Rapporto NSTIC e GCSEC

- 75% degli utenti Internet non vorrebbe creare nuovi account per accedere ad un sito
- 54% degli utenti abbandona un sito o non ritorna se viene richiesta la creazione di una nuova password
- Oltre l'80% degli utenti scelgono come password la stessa utilizzata per la posta elettronica
- In caso di compromissione di una password, lo sforzo richiesto per cambiare la password su tutti i servizi online è estremamente oneroso
- La quasi totalità dei Servizi Web utilizza l'indirizzo di Posta Elettronica come "username"
- L'indirizzo di Posta Elettronica è il sistema più utilizzato per la verifica di identità online, principalmente per consentire di avere un sistema per comunicare con il titolare e per disporre di una modalità di ripristino delle credenziali (cambio password).
- Privacy: l'accesso ai servizi online spesso richiede più Informazioni Personali (PII) di quanto sia realmente necessario, creando archivi potenzialmente esposti a "data breach"
- Gli utenti hanno pochi mezzi per poter controllare la loro identità.
- Facebook sempre più utilizzato come sistema di Single Sign-On. Ogni giorno 600.000 account facebook sono violati (Fonte floridatechonline.com)

Servizio Pubblico di Identità Digitale SPID
Istituzione *DL 69 del 21/6/2013, art. 17-ter*

Art. 17 - *ter*

Sistema pubblico per la gestione
dell'identità digitale di cittadini e imprese

*1. Al comma 2 dell'articolo 64 del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, dopo il primo periodo è inserito il seguente: «Con l'istituzione del sistema SPID di cui al comma 2-*bis*, le pubbliche amministrazioni possono consentire l'accesso in rete ai propri servizi solo mediante gli strumenti di cui al comma 1, ovvero mediante servizi offerti dal medesimo sistema SPID».*

2. Dopo il comma 2 dell'articolo 64 del codice di cui al decreto legislativo 7 marzo 2005, n. 82, come da ultimo modificato dal presente articolo, sono aggiunti i seguenti:

*«2-*bis*. Per favorire la diffusione di servizi in rete e agevolare l'accesso agli stessi da parte di cittadini e imprese, anche in mobilità, è istituito, a cura dell'Agenzia per l'Italia digitale, il sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID).*

*2-*ter*. Il sistema SPID è costituito come insieme aperto di soggetti pubblici e privati che, previo accreditamento*

- L'Art. 17-ter emenda l'art. 2 comma 2 del CAD (DL 7/3/2005 n. 82), aggiungendo 5 nuovi commi
- Diventa obbligatorio l'uso di SPID per l'accesso ai servizi della PA
- L'avviamento dello SPID è a cura dell'AgID
- Modi e tempi di avviamento saranno definiti nel DPCM (2-sexies), da emettere entro il 20/12/2013 (120gg da pubblicazione in Gazzetta Ufficiale)

Il DPCM dovrà essere predisposto con il coinvolgimento di altri Ministri

Art. 17 - *ter*

Sistema pubblico per la gestione
dell'identità digitale di cittadini e imprese

*1. Al comma 2 dell'articolo 64 del codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, dopo il primo periodo è inserito il seguente: «Con l'istituzione del sistema SPID di cui al comma 2-*bis*, le pubbliche amministrazioni possono consentire l'accesso in rete ai propri servizi solo mediante gli strumenti di cui al comma 1, ovvero mediante servizi offerti dal medesimo sistema SPID».*

2. Dopo il comma 2 dell'articolo 64 del codice di cui al decreto legislativo 7 marzo 2005, n. 82, come da ultimo modificato dal presente articolo, sono aggiunti i seguenti:

*«2-*bis*. Per favorire la diffusione di servizi in rete e agevolare l'accesso agli stessi da parte di cittadini e imprese, anche in mobilità, è istituito, a cura dell'Agenzia per l'Italia digitale, il sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID).*

*2-*ter*. Il sistema SPID è costituito come insieme aperto di soggetti pubblici e privati che, previo accreditamento*

- Il Decreto sarà proposto dal Ministro delegato per l'Innovazione Tecnologica e del Ministro per la pubblica amministrazione e la semplificazione (min. D'Alia)
- Il Ministero dell'Economia e Finanze e il Garante per la Privacy dovranno essere interpellati

IDENTITÀ «FORTE»
Le fasi del Ciclo di Vita (1/2)

1	**Verifica informazioni utente e creazione credenziali**	• **verifica** informazioni fornite dal Titolare richiedente • **crea le credenziali** con cui l'utente certificherà l'identità e confermerà i relativi attributi	■ **Verifica documenti di identità** (es.: dati di nascita) ■ Verifica **credenziali professionali** (es.: dati sulla professione o appartenenza ad un'associazione di categoria) ■ (*Conduzione di indagini per verificare l'assenza di condizioni negative (es.: frodi, protesti, conflitti di interesse))* ■ Le credenziali create possono essere di diverso tipo: **user-id e password, PCR, firma digitale, ..**
2	**Fornitura delle credenziali**	Il processo di provisioning garantisce che l**e credenziali generate** nella fase precedente siano **consegnate con certezza** al cliente identificato, che provvede ad attivarle	■ **Acquisizione "diretta"** (di persona) delle credenziali dopo aver presentato la documentazione di riconoscimento ■ **Invio credenziali ad un indirizzo di posta certificata** o ad un device "sicuro" ■ **Attivazione** delle credenziali da un **device "sicuro"** ■ **Attivazione** delle credenziali tramite la **presentazione di informazioni** per l'identificazione

IDENTITÀ «FORTE»
Le fasi del Ciclo di Vita (2/2)

3 Accesso ai servizi

Il Titolare presenta le credenziali ad un "**fornitore di servizi**" per eseguire **l'accesso ai servizi** L'accesso può avvenire anche attraverso diversi siti/ portali

Tipo di attività	Credenziali da presentare: ID + pass	PCR	Firma dig	Token
Autenticazione	✓			(✓)

Non indispensabile in fase di autenticazione

4 Verifica delle credenziali

Il "fornitore di servizi" **verifica le credenziali** (eventualmente previa verifica del "fornitore di identità") ed abilita l'utente all'utilizzo dei servizi in funzione degli attributi dell'identità del cliente

- **Verifica delle credenziali** dell'utente ed abilitazione all'utilizzo dei servizi in funzione degli attributi dell'identità del cliente

5 Utilizzo dei servizi

Il Titolare utilizza i servizi resi accessibili dal "fornitore di servizi"

	Credenziali da presentare: ID + pass	PCR	Firma dig	Token
Servizi transazionali		✓		✓
Sottoscrizione Contratti			✓	

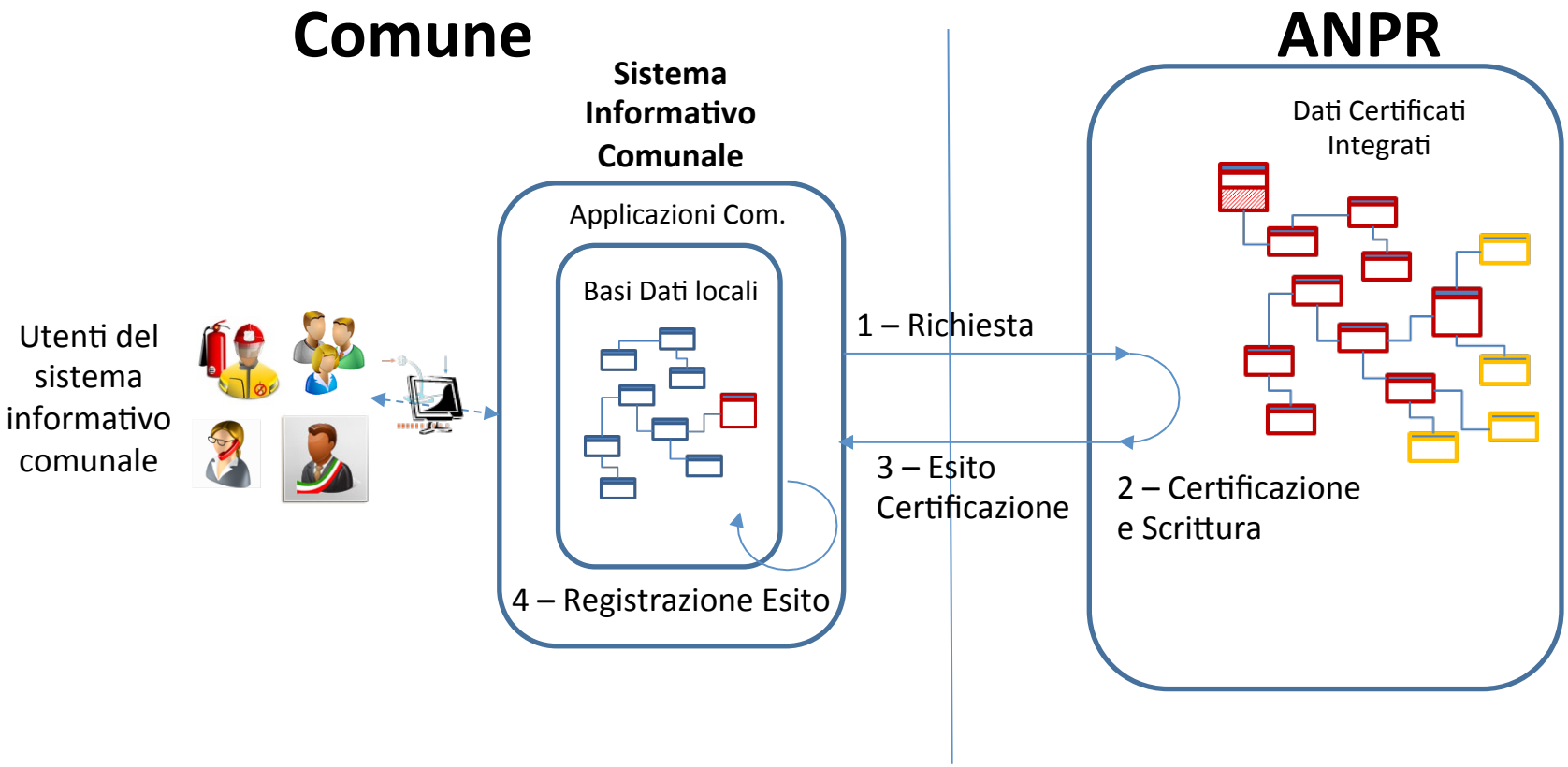
Le modalità di avvio

- **Modalità compatibili con gli adeguamenti necessari:** Sono stati previsti i tempi e le modalità per consentire un efficace adeguamento dei sistemi informativi comunali
- **Periodo di avviamento:** Ogni comune avrà un proprio periodo di "rodaggio" e verifica delle informazioni prima del passaggio
- **Segnalazione e Gestione Anticipata Anomalie:** Le situazioni anomale verranno segnalate con largo anticipo sia su base nazionale che per ogni Comune
- **Monitoraggio della Qualità:** Si adotteranno criteri statistici, modalità di rilevazione ed indicatori (KPI) di verifica incrociata delle informazioni
- **Completamento soluzione anomalie residuali non bloccante:** Eventuali situazioni anomale residuali verrano sanate dai Comuni interessati dopo il passaggio ad ANPR

Modello di Interazione ANPR – S.I. Comunali

Vista di alto livello dei processi di funzionamento

CONCETTUALE

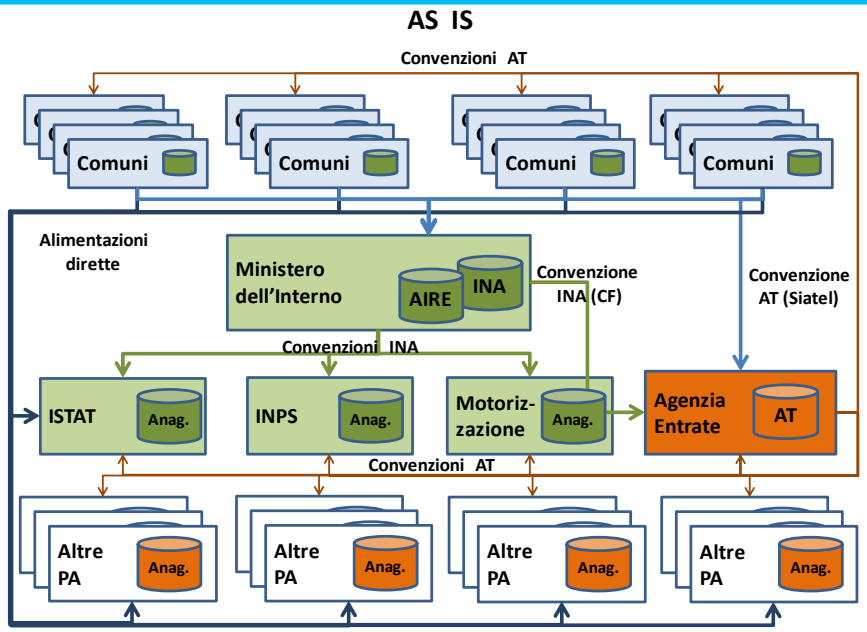


Efficienza della struttura informativa

Esempio circolarità dati anagrafici

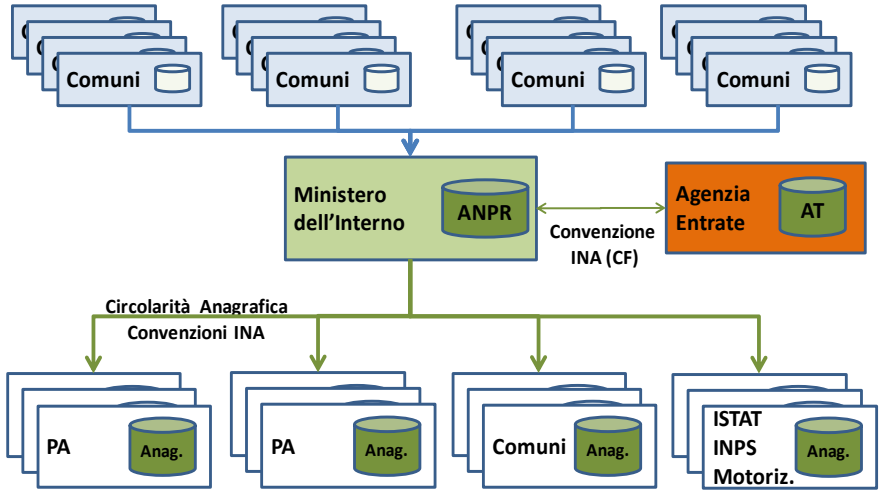
CONCETTUALE

FORUM PA 2014



Modello di Riferimento a "stella"

TO BE



SPID
Domande Frequenti
(FAQ)

SPID - Frequently Asked Questions – FAQ (1/3)

Domanda: Come si diventa Gestore di Identità Digitale o Fornitore di Attributi Qualificati?

Risposta: La società che dispone dei requisiti giuridici e tecnici definiti dal Decreto SPID e dal Regolamento Attuativo emesso dall'Agenzia Per l'Italia Digitale, potrà inoltrare a quest'ultima richiesta di accreditamento. L'Agenzia provvederà ad accreditare la Società, previa sottoscrizione di una convenzione e iscrivendola nel Registro Pubblico di SPID.. La società sarà soggetta a vigilanza da parte dell'Agenzia per l'Italia Digitale.

Domanda: Cosa devono fare i Gestori di Servizi interessati ad aderire a SPID?

Risposta: Dovranno presentare richiesta di accreditamento all'Agenzia per l'Italia Digitale. L'Agenzia provvederà ad accreditare il Gestore di Servizi, previa sottoscrizione di una convenzione e iscrivendolo nel Registro Pubblico di SPID.

Domanda: Come fa un utente a richiedere una Identità SPID?

Risposta: L'Utente interessato a diventare titolare di una Identità SPID potrà rivolgersi ad un qualsiasi Gestore di Identità Digitale accreditato per ottenere una Identità Digitale.

SPID - Frequently Asked Questions – FAQ (2/3)

Domanda: Quale è il processo per il rilascio di una Identità Digitale?

Risposta: Il Richiedente formulerà richiesta ad un Gestore di Identità Digitale Accreditato, il quale procederà con l'attività di verifica, ovvero al riconoscimento de visu del titolare richiedente e al rilascio in modalità sicura di una o più credenziali.

Domanda: Il riconoscimento de-visu è sempre richiesto?

Risposta: No. Se il richiedente possiede già uno strumento di Identità Elettronica associato ad una credenziale di Livello LoA4 (CIE, CNS, TS-CNS, CRS, DU), l'Identità SPID potrà essere rilasciata senza ripetere la verifica de visu, già effettuata per il rilascio dell'Identità Elettronica.

Domanda: Può un soggetto essere titolare di più Identità SPID?

Risposta: Si. Chi dispone di una Identità SPID potrà richiedere ad un altro Gestore d'Identità Digitale una nuova identità, senza effettuare la verifica de-visu.

SPID - Frequently Asked Questions – FAQ (3/3)

Domanda: SPID non rischia di diventare un punto debole che se violato può consentire l'accesso non autorizzato a tutti i Gestori di Servizio aderenti a SPID?

Risposta: No. Gli Identity Provider sono tenuti a rispettare alti standard di Sicurezza, non solo per la protezione del sistema, ma anche per la rilevazione di usi anomali. L'adozione dei livelli LoA 3 e 4 risolvono comunque I più comuni e noti problemi di sicurezza legati al furto d'Identità e all'Impersonificazione.

Domanda: E' possibile per il Gestore di Servizo utilizzare unicamente il servizio di "autenticazione"?

Risposta: Si. Il Gestore di Servizio non interessato a conoscere la vera identità dell'utente, può richiedere al Gestore d'Identità Digitale esclusivamente il servizio di autenticazione. In questo caso è garantita la Pseudonimity, ovvero il Gestore di Servizi non conoscerà l'Identità dell'Utente, ma è possibile la sua identificazione in caso di attività illecite.

Domanda: Quali sono i dati minimi che il gestore d'Identità fornisce ad un Gestore di Servizi?

Risposta: SPID rispetta il principio della minima condivisione. Il Gestore di Servizi determina il numero minimo di attributi necessari per l'accesso al servizio. Il Gestore dell'Identità fornirà gli attributi, previo consenso del Titolare