UN'ARCHITETTURA UNITARIA

PER L'AGENDA DIGITALE

- Il nuovo modello di cooperazione SPC -

Nome del documento.:	**ArchitetturaITPAFinal.doc**	Versione:	**0.6**
Data:	**25 Luglio 2013**	Stato:	**finale**

INDICE

ACRONIMI

AA – Attribute Authority

AAR – Attribute Authority Registry

AR – Authority Registry

ANPR – Anagrafe della Popolazione Residente

ATECO – Attività ECOnomiche

CAD – Codice dell'Amministrazione Digitale (Decreto Legislativo n. 82/2005 e s.m.i.)

CERT – Computer Emergency Response Team

DL – Decreto Legge

D.Lgs – Decreto Legislativo

DPCM – Decreto Presidente del Consiglio dei Ministri

EIF – European Interoperability Framework

EDA – Event Driven Architecture

FOAF – Friend of A Friend

GFID – Gestione Federata delle Identità Digitali

IaaS – Infrastructure as a Service

IT – Information Technology

IP – Internet Protocol

IPA – Indice della Pubblica Amministrazione

IGPEC – Indice dei Gestori PEC

INI-PEC – Indice Nazionale degli Indirizzi di Posta Elettronica Certificata delle imprese e dei professionisti

MPLS – Multi Protocol Label Switching

NAP – Network Access Point

PA – Pubblica Amministrazione

PaaS – Platform as a Service

PEC – Posta Elettronica Certificata

QoS – Quality of Service

QXN – Qualified eXchange Network

SaaS – Software as a Service

SICA – Servizi di Interoperabilità, Cooperazione e Accesso

SOA – Service Oriented Architecture

SOC – Security Operating Centre

SPC – Sistema Pubblico di Connettività

GLOSSARIO

AA (Attribute Authority): Entità designata a certificare tutti o parte degli attributi componenti il profilo di un generico utente.

AAR (Attribute Authority Registry): Registro contenente la relazione fra ruolo e URI del suo certificatore.

AR (Authority Registry): Entità che permette di rintracciare in modo univoco all'interno di SPC i riferimenti agli Identity Provider.

ATECO: Classificazione delle attività economiche.

EIF (European Interoperability Framework): descrive il modo in cui organizzazioni hanno concordato o dovrebbero concordare di interagire l'uno con l'altro, e come gli standard dovrebbero essere utilizzati. Esso fornisce quindi le politiche e le raccomandazioni che formano la base per la selezione degli standard da adottare nell'interazione tra organizzazioni.

EDA: è un modello architetturale che abilita la produzione, la notifica e il consumo di eventi.

FOAF: è un'ontologia che descrive le persone, le loro attività e le relazioni con altre persone.

ONTOLOGIA: è una rappresentazione formale delle informazioni e delle loro interrelazioni.

SOA: è un modello architetturale per la progettazione di sistemi software distribuiti basato sul concetto di servizio, dove servizio è definito come un modulo software che espone un'interfaccia (o contratto) utilizzata per descrivere le funzionalità offerte dal servizio.

1. SCOPO E STRUTTURA DEL DOCUMENTO

Lo scopo del presente documento è quello di introdurre l'architettura IT di riferimento della Pubblica Amministrazione italiana (i.e., il framework SPC definito ai sensi dell'art. 73 del Codice dell'Amministrazione Digitale) presentando un'evoluzione del modello di cooperazione attualmente vigente. Il nuovo modello è in grado di garantire i diversi livelli di interoperabilità così come descritti nell'ambito del framework europeo di interoperabilità: organizzativa, semantica e tecnica.

Il documento evidenzia l'applicabilità del modello a un caso di studio complesso come quello della nuova architettura dell'Anagrafe Nazionale della Popolazione Residente (ANPR) e discute, infine, dei modelli di deployment di mercato che possono essere adottati per mettere in produzione le componenti del modello.

Il documento è strutturato come segue. La sezione 2 introduce il contesto di riferimento e analizza l'intero quadro normativo riferendosi all'agenda digitale europea e alla relativa italiana, al CAD e evidenziando il ruolo del Sistema Pubblico di Connettività – SPC in tale scenario normativo. La sezione 3 dettaglia i requisiti da considerare per la definizione dell'architettura IT di riferimento della Pubblica Amministrazione italiana che è introdotta nella sezione 4 unitamente al modello di cooperazione per l'interoperabilità abilitato da tale architettura. La sezione 5 discute dei modelli di deployment di mercato che possono essere utilizzati al fine di attuare l'architettura. Infine, la sezione 6 conclude il documento presentando un esempio di istanziazione dell'architettura IT presentata nel caso della banca dati di interesse nazionale ANPR – Anagrafe Nazionale della Popolazione Residente.

2. INTRODUZIONE

Dai presupposti e obiettivi dell'Agenda digitale europea, che già costituisce un indirizzo vincolante all'attuazione dell'Agenda digitale italiana, e dalle norme che si sono succedute negli ultimi due anni in materia di amministrazione digitale (Sezione 2.1), emerge la necessità di una visione unitaria e sistemica dell'ICT che possa fare da motore all'economia (digitale) dei prossimi anni. Una visione sistemica e unitaria deve essere capace non solo di definire linee guida e regole tecniche ma assicurare l'omogeneità dei sistemi e delle soluzioni, almeno nel senso di poter efficacemente utilizzare prodotti di mercato e soluzioni indipendenti potendole inter-cambiare, sostituire anche parzialmente, farle evolvere e integrarle senza la necessità di interventi ad hoc o che diventino "legacy" per una ordinata evoluzione. A tale scopo, il mero utilizzo di modelli di computing e di tecnologie innovative o modelli di procurement, da soli non sono però sufficienti. Allo stesso modo, molte politiche di razionalizzazione, certamente utili, se non indispensabili in questo periodo, non hanno la stessa efficacia se gli interventi non fanno riferimento a un preciso modello di cooperazione e a un quadro organico dei componenti e delle linee di intervento. Restano, infatti, ancora alcuni ostacoli di natura organizzativa da superare: la reingegnerizzazione dei processi, la frammentazione delle decisioni di scelta in merito a soluzioni e servizi ICT. I primi si traducono in una perdita di efficacia degli interventi di innovazione, i secondi in una perdita di efficienza. Tali ostacoli vanno superati con politiche di accordi, creando un clima partecipativo, inclusivo e una governance trasparente, con la fermezza che le azioni necessarie alla digitalizzazione del paese non sono più derogabili. Altro importante aspetto da considerare è quello che in alcuni settori il mantenimento e il miglioramento delle prestazioni organizzate fornite dallo Stato e dalle sue articolazioni e autonomie, passa attraverso la digitalizzazione, non essendo più sostenibile (e talvolta efficace dato lo sviluppo delle tecnologie) l'attuale tipo di spesa.

Alla luce delle precedenti osservazioni, ne deriva quindi la necessità di definire un'architettura IT di riferimento così da poter promuovere e attuare gli investimenti più efficaci ed efficienti al fine di dare piena attuazione alla digitalizzazione della Pubblica Amministrazione (PA) e del Paese (da recenti studi si stima che interventi nella PA coinvolgono circa il 50% del PIL nazionale) [studi McKyney].

In tale scenario, il legislatore ha inteso creare l'Agenzia dell'Italia Digitale, che nasce non soltanto con l'intento di migliorare le sinergie tra i diversi attori che compongono il quadro delle competenze di indirizzo, coordinamento e realizzazione delle infrastrutture digitali del Paese, ma ha affidato all'Agenzia ulteriori e cogenti compiti (si veda le successive sezioni). Non di meno il quadro legislativo ha inteso definire meglio i ruoli di altri attori, rafforzando sia quello della SOGEI, alla quale vengono affidati la realizzazione e la gestione di tutti i progetti inerenti al Ministero dell'Economia e Finanze (aprendo la possibilità ad un utilizzo della SOGEI in altri ambiti critici di valenza nazionale) sia quello della Consip, alla quale vengono affidate tutte le procedure di acquisiti del suddetto Ministero e ne vengono potenziate le azioni in termini di centrale di committenza. Tali soggetti, unitamente alle commissioni già previste dalla norma (e.g., art. 17 del CAD, art. 79 del CAD, art. 20 DL 179/2012) e ai CIO delle PA, agli interlocutori principali della PA (banche, utilities, professionisti), al mercato, hanno il compito primariamente di condividere modelli e piani di sviluppo. Non di meno, i modelli di open government, i social network e i media pongono gli utenti della PA in un ruolo profondamente diverso rispetto al passato dove l'unica possibilità degli utenti era quella di chiedere e ricevere un servizio. La

disponibilità di tecnologia presso gli utenti finali, oramai non più solo presso i "nativi digitali", deve rappresentare un elemento di valutazione e di relazione delle azioni di digitalizzazione.

Un modello di riferimento, come insieme coordinato di indirizzi, regole tecniche e strumenti, è già in parte previsto dal CAD e dal recente DL 179/2012 (in quest'ultimo caso per esempio per ciò che concerne le comunità intelligenti). Il modello può costituire quel collante per l'attuazione delle politiche, anche industriali sull' ICT andando oltre le stesse PA.

Nell'ambito del CAD, le definizioni che riguardano il Sistema Pubblico di Connettività - SPC consentono di ridefinirne il modello architetturale e i settori di intervento, rimanendo nel solco delle macro-categorie definite dall'art. 72 del CAD, in maniera tale da soddisfare le esigenze prospettabili nello scenario delineato. Allo stesso tempo, tale sforzo di rifocalizzazione e le stesse direttrici di intervento previste per SPC possono essere utilizzate come modello per altri ambiti di azione previste dal nuovo scenario normativo (come ad esempio nel caso delle comunità intelligenti).

2.1. Quadro normativo

Il quadro normativo di riferimento coinvolge tre principali driver: l'agenda digitale europea, l'agenda digitale italiana, definita allo scopo di portare l'Italia alla piena attuazione di quella Europea, e il rinnovato Codice dell'Amministrazione Digitale (D.lgs n. 82/2005) che include al suo interno una serie di provvedimenti definiti dall'agenda digitale italiana.

Nel seguito si evidenziano i principali interventi nei tre riferimenti normativi suddetti e si discute dello specifico ruolo del Sistema Pubblico di Connettività e Cooperazione (SPC) in tale contesto.

2.1.1. L'agenda digitale europea

La Commissione europea ha lanciato nel marzo 2010 la strategia Europa 2020 [1] per poter uscire dalla crisi e preparare l'economia dell'unione europea alle sfide del prossimo decennio. La digital agenda europea [2] è una delle sette iniziative cardine della strategia. Essa mira a stabilire il ruolo chiave delle tecnologie dell'informazione e della comunicazione per raggiungere gli obiettivi che l'Europa si è prefissata per il 2020. Secondo la digital agenda, "*grazie all'evoluzione in atto nel settore dell'elettronica di consumo, i confini tra i diversi dispositivi digitali stanno scomparendo. I servizi convergono e si spostano dal mondo fisico a quello digitale, universalmente accessibile su qualsiasi dispositivo, che si tratti di smartphone, tablet PC, computer, radio digitali o televisori ad alta definizione. Si prevede che entro il 2020 i contenuti e le applicazioni digitali saranno forniti quasi interamente online.*".

L'agenda digitale si compone di sette pilastri ("pillar"). A ognuno dei pilastri sono associate delle azioni, che sia la Comunità Europea sia i paesi membri, per i sistemi di loro competenza, devono intraprendere per rendere operativi i relativi pilastri. Un vasto sottoinsieme di tali azioni impattano la modellazione della possibile architettura unitaria per l'agenda digitale che l'Italia deve promuovere e utilizzare. Così, per la realizzazione di un mercato unico digitale, azioni chiave riguardano l'apertura di dati per il riuso (action 3) e l'implementazione di leggi e piattaforme che abilitano un unico e-commerce (action 10). Per l'interoperabilità e la standardizzazione, è cruciale allineare i framework nazionali di interoperabilità all'European Interoperability Framework (EIF) (action 24 e 26), e promuovere in maniera sempre più crescente l'utilizzo di tecnologie standard e aperte (action 22). Per quel che riguarda la fiducia e la sicurezza online, si richiede che i paesi membri predispongano piattaforme nazionali per combattere

attacchi di sicurezza e piattaforme utilizzate da una rete di CERT per contrastare in maniera collaborativa attacchi sempre più complessi, distribuiti nel tempo e nello spazio che coinvolgono non solo meri aspetti di rete ma anche più applicativi (action 38 e 41). Per diminuire il digital divide, gli stati membri si impegnano a fornire Siti Web del settore pubblico che siano completamente accessibili, e in generale servizi pubblici usabili, anche da persone con disabilità. Per quanto riguarda invece il ruolo dell'information and communication technology (ICT) nei servizi pubblici, gli stati membri devono impegnarsi (i) alla realizzazione di servizi per la sanità elettronica che siano sempre più accessibili a tutti gli attori coinvolti (action 75), (ii) alla realizzazione di meccanismi di identificazione e autorizzazione anche transfrontalieri (action 83), e all'erogazione continua di servizi e-government di alta qualità che siano interoperabili anche con analoghi servizi a livello europeo (action 84 e 89).

A integrazione dei pilastri discussi, lo scorso dicembre la Commissione Europea ha dettagliato le nuove priorità digitali per il 2013-2014 [3]. Tra esse, di particolare rilevanza ai fini della definizione di un'architettura IT di riferimento per l'agenda digitale italiana, è l'accelerazione dell'adozione del cloud computing nel settore pubblico e della relativa dismissione della miriade di attuali "datacenter" chiusi nazionali. Tale priorità, se opportunamente recepita, nel contesto europeo è considerata un'azione in grado di dare un aiuto sostanziale alla creazione del più grande mercato ICT basato sul cloud, capace di favorire l'apertura del mercato unico, risparmi sulla spesa pubblica e l'attuazione dell'interoperabilità.

2.1.2. *L'agenda digitale italiana e il CAD*

Nonostante il forte orientamento all'uso pervasivo delle tecnologie dell'informazione e comunicazione dell'agenda digitale europea, "*l'Europa soffre di una crescente carenza di competenze professionali nel settore delle tecnologie dell'informazione e della comunicazione e di analfabetismo digitale. Queste carenze escludono molti cittadini dalla società e dall'economia digitale e limitano il forte effetto moltiplicatore sull'aumento della produttività che deriverebbe dall'adozione delle tecnologie dell'informazione e della comunicazione*" [10]. In particolare, secondo il rapporto ISTAT "Cittadini e nuove tecnologie" del 2011 [12], l'Italia in ambito europeo si colloca al 22° posto per diffusione delle tecnologie digitali e da uno studio del Ministero dello Sviluppo Economico il 4,8% della popolazione residente (quindi circa 2,9 milioni di cittadini) evidenzia un divario digitale di base (disponibilità di una connessione a una velocità pari almeno a 2 Mbps o su rete fissa o su Banda Larga mobile) [11].

Il Governo Italiano, pertanto, per rispondere alle istanze poste dall'agenda digitale europea come prima descritto, ha istituito lo scorso anno una cabina di regia il cui compito era quello di coordinare le azioni delle amministrazioni centrali e territoriali e fissare le linee guida di una propria Agenda Digitale. Nasce quindi l'Agenda Digitale Italiana [4] e l'organo responsabile della sua implementazione, ossia l'Agenzia per l'Italia Digitale (ai sensi degli artt. 19, 20, 21, 22 del DL n.83/2012), considerata anche "*autorità di riferimento nazionale nell'ambito dell'Unione europea e internazionale*".

L'agenda digitale italiana si fonda sui seguenti temi dell'innovazione: banda larga e ultralarga, cloud computing, open data ed e-government, comunità intelligenti e inclusione digitale. I risultati dello studio di questi temi hanno dato origine all'insieme di provvedimenti del DL n.179/2012. Alcuni dei provvedimenti del decreto inseriscono nello scenario di innovazione italiano elementi nuovi come per esempio la piattaforma nazionale delle comunità intelligenti e il fascicolo sanitario elettronico (FSE), altri invece si configurano come modifiche ad articoli (e in generale principi) già precedentemente

sanciti dal Codice dell'Amministrazione Digitale (D.lgs n. 82/2005). In particolare, le modifiche riguardano: le modalità di accesso ai dati (open data), le basi dati di interesse nazionale (con l'individuazione di quelle critiche), il domicilio digitale del cittadino e il documento unico, l'indice nazionale delle PEC delle imprese e dei professioni, la riprogettazione dell'Indice della Anagrafi con la nascita di una base di dati di interesse nazionale che racchiuda tutti i dati relativi alla residenza dei cittadini (Anagrafe Nazionale della Popolazione Residente – ANPR, da istituire presso il Ministero dell'Interno), per citare alcune.

Per promuovere lo sviluppo di progetti connessi alla realizzazione dell'agenda digitale italiana, l'Agenzia per l'Italia Digitale è chiamata a raccogliere proposte di imprese singole o in partenariato tra di loro, eventualmente in associazione con organismi di ricerca, valutandole dal punto di vista tecnico-scientifico e dal punto di vista finanziario,. In quest'ultimo caso, l'uso congiunto di contributi pubblici e privati e fondi comunitari potrà essere considerato al fine di facilitare lo sviluppo di progetti che possano incidere in maniera significativa sui processi di integrazione e innovazione.

Codice dell'Amministrazione Digitale. Nel Codice dell'Amministrazione Digitale (CAD) emanato nel 2005 venivano già date indicazioni su come il complesso processo di digitalizzazione e di interoperabilità tra le pubbliche amministrazioni sarebbe potuto avvenire al fine di garantire una più efficiente ed efficace azione pubblica. Così, per esempio, si prevedeva che i pagamenti potevano anche essere svolti per via telematica o che i siti web delle pubbliche amministrazioni dovevano già contenere tutte quelle informazioni (e.g., l'organigramma, l'articolazione degli uffici, l'elenco delle tipologie di procedimento svolte da ciascun ufficio, le scadenze dei procedimenti, gli indirizzi di posta elettronica) necessarie ai cittadini e alle imprese per facilitare il "contatto" con le pubbliche amministrazioni.

Nel dicembre del 2010, sulla base della delega contenuta nella legge n. 69/09 sono stati effettuati interventi di modifica del CAD, che hanno dato vita al D.Lgs. n. 235, per rendere lo stesso CAD, meno di principio e più efficace. Tali integrazioni e modifiche si sono rese necessarie per rispondere al verificarsi di un insieme di eventi che non potevano essere trascurati nella realizzazione del futuro sistema strategico di digitalizzazione delle pubbliche amministrazioni. Vengono quindi considerati (i) sia la rapida evoluzione delle tecnologie presenti sul mercato, (ii) sia, di conseguenza, le rinnovate esigenze/aspettative dei cittadini e imprese che richiedono di poter dialogare con un apparato pubblico snello, veloce e meno oneroso e di poter usufruire di servizi sfruttando qualunque mezzo digitale connesso a Internet (e.g., non più solo telefonia fissa ma anche mobile), (iii) sia il recepimento della riforma Brunetta (D.Lgs n. 150 del 2009) che introduce elementi quali premialità, trasparenza e responsabilizzazione dei dirigenti che si ripercuotono su diverse norme del CAD più stringenti rispetto al passato in cui, se da un lato, amministrazioni virtuose vengono incentivate con la possibilità di quantificare e riutilizzare i risparmi ottenuti grazie alle tecnologie digitali, dall'altro però prevedono sanzioni per quelle inadempienti.

2.1.3. SPC nel nuovo quadro normativo

Nel CAD trova altresì spazio il Sistema Pubblico di Connettività definito come *"l'insieme di regole tecniche, infrastrutture condivise e servizi di base, conformi alle regole per la realizzazione di servizi interoperabili in rete"*.

Sebbene sussista ancora una prevalente associazione storica di SPC agli aspetti di rete, e ancora di più ai contratti per la fornitura dei servizi di rete, una rinnovata visione dello stesso è

tuttavia proposta dal CAD e dalle nuove norme sull'agenda digitale italiana, in cui maggiore enfasi viene data al contesto interoperabilità e cooperazione a livello applicativo, all'utilizzo sempre maggiore di servizi nazionali condivisi di supporto come presupposto per l'erogazione di servizi applicativi di e-government evoluti e alla definizione di regole tecniche e linee guida a cui le Pubbliche Amministrazioni devono uniformarsi. A tal riguardo, è importante notare che molti articoli del CAD fanno riferimento a SPC per l'attuazione di quegli stessi provvedimenti, **trasformando così SPC nell'architettura IT per l'interoperabilità della Pubblica Amministrazione italiana, comprendente un framework di regole e linee guida e una enterprise architecture dei sistemi informativi di tutta la PA.**

Nel CAD l'utilizzo delle tecnologie ICT presenti sul mercato assume un ruolo predominante per realizzare SPC e per portar a termine le diverse fasi del processo amministrativo già avviate nel passato, ma che richiedono di essere completate e concretizzate. In particolare, esse sono lo strumento necessario per:

- migliorare i rapporti di interscambio tra pubbliche amministrazioni e imprese e cittadini;
- effettuare *pagamenti elettronici* attraverso l'ausilio di qualsiasi strumento digitale, così come previsto dall'art. 5 del CAD;
- attuare in modo concreto il processo di *dematerializzazione* e *conservazione* dei documenti (art. 42);
- gestire interamente il *protocollo informatico* (art. 41 del CAD) con possibilità di realizzare fascicoli tra più amministrazioni;
- migliorare l'accesso ai servizi in rete attraverso anche l'ausilio di meccanismi di *identificazione federata* e lo scambio dei dati, mediante l'uso di *banche dati di interesse nazionale* (art. 60 del CAD), così che il cittadino possa evitare di fornire più di una volta i propri dati personali e accedere a una più vasta pletora di servizi disponibili;
- incrementare i livelli di *sicurezza* dei sistemi informativi delle pubbliche amministrazioni, rispondendo anche se necessario in maniera tempestiva ed efficace alle varie minacce e attacchi di sicurezza (artt. 50, 51 del CAD).

Anche nel contesto dell'Agenda Digitale Italiana (DL n. 179/2012) il ruolo di SPC viene rafforzato. Come prima menzionato, il decreto si sviluppa su una serie di interventi che possono concretizzarsi grazie alla presenza di un'architettura IT di riferimento unitaria. Questo si riscontra:

- nell'ambito *delle identità digitali*, dove una visione organica e unitaria come proposta nel contesto SPC (si veda a tal proposito il modello di gestione federata delle identità digitali (GFID) [5]) è ora richiesta e può essere attuata con maggiore semplicità grazie ai recentissimi interventi normativi del CAD previsti agli artt. 28, 65 e 6-bis. In quest'ultimo caso, in particolare, si istituisce l'Indice Nazionale degli Indirizzi di Posta Elettronica Certificata delle imprese e dei professionisti (i.e., INI-PEC) presso il Ministero dello Sviluppo Economico; tale indice può essere utilizzato per accertare il ruolo dei professionisti ma ulteriori interventi normativi al riguardo si rendono necessari;
- nell'ambito della *piattaforma delle comunità intelligenti,* dove i servizi di supporto nazionali SPC possono essere riutilizzati e le regole tecniche e linee guida per l'interoperabilità, per il riuso e scambio di dati devono essere promosse (alcune raccomandazioni alle PA per la definizione di

un'architettura unitaria per le comunità intelligenti dove emerge il ruolo di SPC sono state pubblicate lo scorso anno dall'Agenzia per l'Italia Digitale [7]);

- nell'ambito di servizi settoriali verticali (e.g., fascicolo elettronico sanitario) dove le regole tecniche e linee guida definite nel contesto SPC dovranno essere recepite, pur salvaguardando ed utilizzando gli ampi standard settoriali e i modelli e best practices più diffusi;
- nell'ambito delle *basi di dati di interesse nazionali* dove è necessario (i) aggiornare la lista di quelle attualmente previste all'art. 60 del CAD con quelle incluse all'interno DL n.179/2012, come ad esempio l'Archivio Nazionale dei numeri civici e delle strade urbane, l'Anagrafe Nazionale della Popolazione Residente, (ii) definire le caratteristiche generali comuni in termini di gestione e fruizione da parte di altre PA, ivi inclusi gli elementi di sicurezza e continuità di servizio, le interfacce da realizzarsi e gli schemi di convenzione standard (per adesione) e (iii) ampliare tale numero in maniera da rispondere alle esigenze di costituire un insieme di sistemi informativi e basi di dati di primaria importanza nazionale. **A tal riguardo, è importante evidenziare che l'Agenzia per l'Italia Digitale, nel dare attuazione alle previsioni normative di cui all'art. 2-bis del DL n.179/2012, ha recentemente definito i criteri per individuare, nell'ambito delle basi dati di interesse nazionale, quelle *critiche* indicando altresì i requisiti nell'ambito SPC per l'aggiornamento delle stesse sulla base dello standard internazionale ISO/IEC 25012 "Data Quality Model"[13], standard per cui si è avviato l'iter di traduzione in lingua italiana;**
- nell'ambito *dei dati aperti* dove è necessario definire linee guida nazionali (come evoluzione di quelle già prodotte nel contesto SPC sull'interoperabilità semantica attraverso i Linked Open Data [6]) che specificano le modalità operative (indicazione degli standard tecnici e delle ontologie e vocabolari da utilizzate per descrivere i dati aperti, quali tipologie di dati aprire, tempi) che le Pubbliche Amministrazioni dovranno seguire al fine di produrre e pubblicare dati aperti interoperabili. **A tal riguardo, si sottolinea come l'Agenzia abbia già provveduto a dare attuazione, per l'anno 2013, alle disposizione contenute all'art. 9 del DL n. 179/2012 sui dati di tipo aperto, presentando alla Presidenza del Consiglio dei Ministri un'agenda nazionale sulla valorizzazione del patrimonio informativo pubblico (in attesa di approvazione) e predisponendo le linee guida nazionali su tale valorizzazione, anch'esse relative all'anno 2013 (esse saranno pubblicate con delibera del Direttore Generale entro la fine di Luglio 2013);**
- nell'ambito dei *Datacenter* dove devono essere definiti i requisiti di servizio e i livelli minimi di qualità, secondo quanto stabilito nel contesto SPC, anche in funzione dei servizi finali erogati. **A tal riguardo è importante sottolineare che l'Agenzia ha avviato una collaborazione con la Fondazione Ugo Bordoni al fine di acquisire i dati relativi ai centri elaborazioni dati delle Pubbliche Amministrazioni italiane. Tale collaborazione ha già portato a termine la prima fase di rilevazione dei dati grazie alla quale l'Agenzia procederà con la stesura di linee guida nazionali e di un piano triennale di razionalizzazione da presentare alla Presidenza del Consiglio dei Ministri per l'emanazione di un DPCM entro la fine del 2013.**

3. REQUISITI

Data la natura sistemica che si vuole attuare grazie alla definizione dell'architettura IT della Pubblica Amministrazione italiana, si possono definire un insieme di categorie di requisiti generali da soddisfare. Tali requisiti sono:

- **Affidabilità**: può essere declinata negli aspetti che attengono alla sicurezza, alla continuità di funzionamento e alla qualità;
- **Integrabilità**: può essere declinata negli aspetti che attengono ai processi organizzativi, ai servizi tecnologici (a tutti i livelli dello stack tecnico) e informatici; essa deve riguardare anche fonti esterne strutturate e non, media e sensori;
- **Flessibilità**: può essere declinata come capacità di (i) rendere i sistemi comunicanti, (ii) preservare contesti locali e preesistenti, (iii) includere agevolmente nuove tecnologie;
- **Governace**: può essere declinata come gli indirizzi costanti attraverso il monitoraggio e l'accountability.

A questi si aggiungono ulteriori requisiti specifici che possono essere riassunti come segue.

- **Servizi efficaci, efficienti, proattivi e "user-centric":** gli stakeholder richiedono servizi efficaci ed efficienti, tagliati sui bisogni specifici, proattivi e in grado di rispondere rapidamente anche a esigenze nuove e impreviste. Così come precedentemente menzionato, l'utilizzo sempre più massiccio di Internet fa sì che gli stakeholder si aspettino nel prossimo futuro di poter usufruire di servizi in grado di consentirgli di eseguire tutti i passi di un procedimento amministrativo, che possa includere anche un eventuale pagamento finale della prestazione, senza dover necessariamente fare file presso sportelli pubblici ma utilizzando gli strumenti tecnologici in loro possesso, ovunque si trovino. Nel recente quadro normativo che ha visto l'entrata in vigore del decreto n. 179, convertito con la legge n. 221 del 18 dicembre del 2012, sull'agenda digitale italiana tali requisiti emergono chiaramente nelle specifiche declinazioni di servizi per la sanità digitale, per la scuola digitale e la giustizia digitale ad esempio.
- **Multicanalità:** è sempre più diffuso l'utilizzo da parte degli stakeholder di strumenti anche mobili per l'accesso a servizi in rete. Tale scenario è destinato a consolidarsi nei prossimi anni. Nell'ottica della definizione dell'architettura IT della PA (Sezione 4) risulta importante considerare la natura *pervasiva* e *ubiqua* che i servizi applicativi possono assumere, così come anche previsto dall'art. 12 del CAD che espressamente dichiara che le "*pubbliche amministrazioni operano per assicurare l'uniformità e la graduale integrazione delle modalità di interazione degli utenti con i servizi informatici, ivi comprese le reti di telefonia fissa e mobile in tutte le loro articolazioni da esse erogati, qualunque sia il canale di erogazione, nel rispetto della autonomia e della specificità di ciascun erogatore di servizi.*"
- **Usabilità e accessibilità:** l'usabilità e l'accessibilità dei servizi applicativi, offerti attraverso svariati canali, e dei documenti informatici prodotti nell'ambito della pubblica amministrazione diventa un obiettivo importante da indirizzare, così come anche definito delle recenti modifiche apportate al CAD in cui, per esempio, all'articolo 23-ter si specifica espressamente che i documenti informatici "*devono essere fruibili indipendentemente dalla condizione di disabilità personale, applicando i criteri di accessibilità definiti dai requisiti tecnici di cui all'articolo n. 11 della legge 9 gennaio 2004,*

n. 4".

- **E-gov dinamico, razionalizzazione e flessibilità:** le PA, per incrementare la fiducia che i cittadini e le imprese possono avere nei loro confronti, devono saper progettare in maniera concreta sistemi IT *che siano più dinamici*, ossia capaci di soddisfare rapidamente le rinnovate esigenze degli utenti finali, e che possano semplificare notevolmente l'attuale processo burocratico al quale gli utenti finali sono sottoposti ogni qual volta interagiscono con una pubblica amministrazione. Infine, la razionalizzazione delle risorse e dei numerosi centri di calcolo dislocati in varie PA, il più delle volte non interoperabili tra loro, in un periodo di crisi economica e ottica di garantire e promuovere l'interoperabilità e la cooperazione tra PA, diventa uno dei pilastri per la definizione dell'architettura IT di riferimento.
- **Inter-settorialità e coordinamento:** in una logica di sistema, l'architettura IT di riferimento deve poter abilitare lo sviluppo di un ambiente *collaborativo* e *pervasivo* capace di supportare la cooperazione tra diversi settori (e.g., e-health, e-payment, e-procurement), in un contesto digitale fortemente integrato. L'intersettorialità, che caratterizza tra gli altri la definizione di alcuni asset importanti dell'agenda digitale italiana come per esempio le comunità intelligenti, porta maggiore efficienza nei servizi, risparmi e qualità, facendo crescere la fiducia del cittadino verso l'impiego di servizi digitali. In tale logica, tutti i livelli istituzionali devono essere tenuti in considerazione; si dovrà quindi consentire un *coordinamento tra Pubbliche Amministrazioni Centrali (PAC) e Pubbliche Amministrazioni Locali (PAL)* stabilendo accordi generali tra le entità coinvolte e non specifici a un singolo e limitato contesto applicativo.
- **Sicurezza:** requisito non funzionale importante è la necessità di garantire un livello di sicurezza minimo prestabilito tale da abilitare nell'ambito dell'architettura IT di riferimento una cosiddetta "*rete trusted*" per i soggetti che ne fanno parte (cfr. DPCM 1/4/2008 art. 11 comma 3). Conseguenza importante di tale scelta è che ciascuno dei soggetti interconnessi è chiamato a far sì che i propri sistemi assicurino almeno il livello di sicurezza minimo prestabilito. Per raggiungere tale obiettivo è necessario in primo luogo concordare un insieme di regole di sicurezza e di riservatezza nel trattamento di informazioni sensibili rispettate da tutte le componenti dell'architettura. Infine, un opportuno sistema avanzato di *cyber intelligence* in grado di rilevare, ma anche e soprattutto rispondere in maniera tempestiva alle minacce di sicurezza di ogni tipo (e.g., attacchi informatici di rete e applicativi, frodi) a cui i vari sistemi ICT sono oggigiorno quasi quotidianamente sottoposti è un obiettivo auspicabile nell'ottica della progettazione della nuova architettura IT della PA e del suo governo, pur nel rispetto dell'autonomia dei sistemi di sicurezza impiegati da ciascun soggetto e possibilmente in stretta cooperazione anche con organismi internazionali di controllo.
- **Qualità e certificazione dei dati:** nell'abilitare una piena cooperazione tra PA è necessario far sì che sia garantito un elevato livello di qualità dei dati scambiati. Tale obiettivo si può raggiungere solo attraverso l'impiego di un modello e schema comune da utilizzarsi nelle fasi di interscambio tra PA e tale da consentire loro di "dialogare" facilmente facendo riferimento effettivamente allo stesso dato. Le copie di dati oltre a costituire un costo di gestione rappresentano un elemento di inefficienza per il sistema.
- **Modalità di accesso unificato:** gli utenti sono attualmente in possesso di diverse *identità digitali* che utilizzano tipicamente per accedere a una serie di servizi offerti loro online. Tali utenti possono essere sia i dipendenti della Pubblica Amministrazione, sia gli operatori di settore, sia tutti i cittadini. In tale scenario, obiettivo primario è dare la possibilità agli utenti di accedere a

servizi applicativi in maniera sicura, affidabile e in *modalità unificata, i.e., Single Sign On (SSO)* dove l'inserimento delle proprie credenziali avviene una sola volta. In questo senso risulta fondamentale attribuire dei profili di accesso agli utenti sulla base del modello Role-Based Access Control (RBAC) per poter *assegnare dei permessi* in relazione ai loro ruoli (o qualifiche) e *tracciare* le attività degli utenti stessi verificandone la validità rispetto ai permessi a loro attribuiti. Se opportunamente soddisfatti, tali requisiti possono migliorare la percezione di qualità e fiducia nei servizi delle pubbliche amministrazioni, evitando duplicazioni di informazioni, fonti di inefficienza e di insicurezza. Infine si evidenzia che in tale ambito, diverse soluzioni sono già state adottate, soprattutto a livello regionale; pertanto, è auspicabile riutilizzare tali soluzioni o quantomeno garantire un certo grado di retro compatibilità con le stesse.

- **Modularità e riuso del software:** per "riuso del software" si intende la possibilità per una Pubblica Amministrazione Centrale o Locale di riutilizzare gratuitamente i programmi applicativi realizzati esclusivamente da o per conto di un'altra PA, adattandoli alle proprie esigenze. Bisogna quindi evitare, qualora possibile, un'implementazione "by scratch" dei servizi stessi e al contrario promuovere e incentivare soluzioni implementative modulari, in cui vi sia una chiara definizione delle interfacce dei servizi possibilmente espresse attraverso standard aperti e comuni e in cui "*i programmi appositamente sviluppati per conto e a spese dell'amministrazione siano facilmente portabili su altre piattaforme*" (art. 69 del CAD). I requisiti di modularità, riuso o condivisione del software esistente, se opportunamente soddisfatti, risultano essere fondamentali per riorientare i flussi economici verso settori non ancora coperti da informatizzazione e per rispondere effettivamente agli obiettivi prima citati di razionalizzazione della spesa pubblica.

Si ritiene che uno scenario così ambizioso debba essere implementato con gradualità, consenso, misurazioni e debba prevedere una serie di azioni, anche di sussidiarietà, non ultime la formazione e la comunicazione, calate in una contesto sistemico e unitario.

4. ARCHITETTURA IT DI RIFERIMENTO

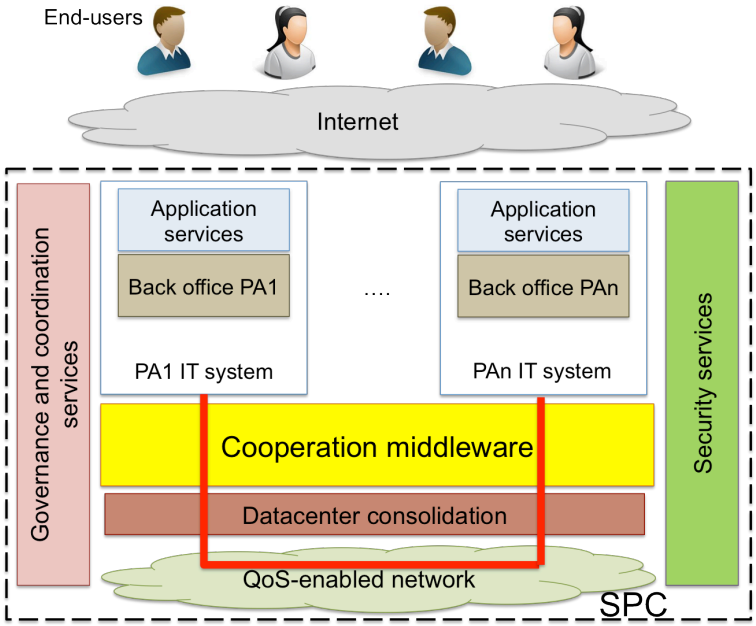

Figura 1: Architettura IT di riferimento: componenti principali

La Figura 1 mostra una "vista" di alto livello dell'architettura IT di riferimento, ossia del Sistema Pubblico di Connettività – SPC (**di seguito quindi si usano i termini "architettura IT di riferimento", o semplicemente "architettura", e "SPC" in maniera equivalente**) con le sue principali componenti o aree di intervento. La definizione dell'architettura è guidata dai seguenti quattro principi basilari:

- **Governo:** rappresenta la possibilità di esercitare una governance, anche distribuita sui territori, in grado di guidare gli stakeholder nel perseguire efficacemente obiettivi di economicità e di concorrenza del mercato, e di promuovere l'innovazione e l'uso di tecnologie standard e aperte.
- **Interoperabilità**: in linea con la definizione di interoperabilità così come definita nel contesto dell'European Interoperability Framework (EIF), rappresenta l'abilità che i diversi stakeholder hanno di interagire, in maniera "seamless" e con garanzie di qualità ed efficacia, per il raggiungimento di obiettivi comuni e concordati reciprocamente, condividendo informazione e conoscenza attraverso i loro processi di business e lo scambio di dati tra i diversi sistemi IT.
- **Federabilità**: rappresenta la possibilità che i diversi stakeholder hanno di associarsi, pur mantenendo la propria autonomia, al fine di condividere dati e processi di business attraverso l'interoperabilità.
- **Sicurezza/Privacy**: rappresenta la possibilità di coordinare la condivisione dei dati e dei processi attraverso l'interoperabilità nel pieno rispetto di requisiti di sicurezza e privacy.

Come evidenziato in Figura 1, l'architettura consente ai diversi sistemi IT delle Pubbliche

Amministrazioni italiane, che erogano servizi applicativi utilizzati da utenti finali attraverso la rete Internet, di cooperare mediante l'ausilio di un opportuno strato middleware. Tale middleware abilita un modello di cooperazione necessario per garantire l'interoperabilità, come prima definita, mascherando l'eterogeneità dei livelli sottostanti. I sistemi IT delle PA e il middleware di cooperazione utilizzato dalle stesse per abilitare interoperabilità nell'inter-scambio di dati e conoscenza sono dispiegati in datacenter consolidati e opportunamente federati mediante meccanismi offerti dal livello di datacenter consolidation mostrato in Figura 1. I vari datacenter delle PA sono tra loro connessi mediante l'ausilio di una rete, ossia la rete SPC, che offre garanzie di qualità del servizio (QoS) "end-to-end" e un adeguato livello di sicurezza.

A supporto del modello di cooperazione per l'interoperabilità dei sistemi IT delle Pubbliche Amministrazioni e dei livelli infrastrutturali sottostanti, l'architettura IT di riferimento include un insieme di servizi di sicurezza, di governance e coordinamento. Tutti gli elementi principali dell'architettura sono descritti nel dettaglio nelle successive sezioni.

4.1. Attori principali

E' possibile individuare due categorie principali di stakeholder che intervengono nella definizione dell'architettura prima introdotta: **utenti** e **soggetti di sistema**.

Gli **utenti** sono i soggetti che *non* concorrono alla vera e propria costituzione dell'architettura ma che *fruiscono* dei servizi offerti dalla stessa. Fanno parte di questa categoria i seguenti soggetti:

- i cittadini e professionisti: come indicato nell'art. 3 comma 1 del CAD, i cittadini hanno diritto a ottenere l'uso delle tecnologie telematiche nelle comunicazioni con la PA e con i gestori di pubblici servizi;
- le imprese private: l'art. 3 comma 1 del CAD sancisce gli stessi principi di cui al precedente punto per le imprese private;

I **soggetti di sistema** sono tutti quei soggetti che concorrono alla costituzione e alla governance dell'architettura IT di riferimento. Essi possono interoperare e al tempo stesso associarsi per condividere i propri dati e processi di business al fine di definire servizi integrati tra più soggetti di sistema. Rientrano in tale categoria:

- le PA: tutte le Pubbliche Amministrazioni così come definite all'art. 2 comma 2 del CAD, che potrebbero mettere a disposizione ad altre PA servizi, software e risorse computazionali (anche nell'ottica del rispetto dei requisiti di riuso del software prima introdotti e chiaramente identificati e ridefiniti dal DL n. 179/2012 per ciò che concerne l'art. 69 del CAD);
- le imprese ICT che operano sul mercato: Internet Service Provider o Application Service Provider;
- i gestori di servizi pubblici e i soggetti che perseguono finalità di pubblico interesse (e.g., banche, poste);
- gli organi preposti alla governance: tutti quegli organismi di attuazione e controllo preposti

all'intero governo dell'architettura. In particolare, il governo è affidato alla Commissione di Coordinamento SPC i cui compiti sono definiti all'art. 79 del CAD. Infine, tra gli organismi preposti alla governance rientrano anche l'Agenzia per l'Italia Digitale in qualità di erogatore di servizi di supporto per la cooperazione tra i sistemi IT delle PA e le Regioni relativamente alla loro autonomia locale.

4.2. Modello di cooperazione per l'interoperabilità

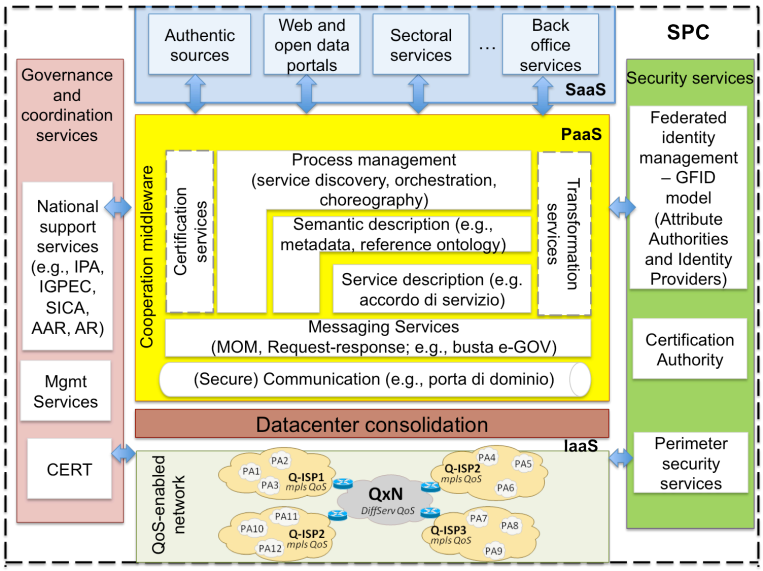

Figura 2: Modello di cooperazione per l'interoperabilità

Il modello di cooperazione per l'interoperabilità (Figura 2) abilita un'architettura *orientata ai servizi*. Esso è utilizzato dalle Pubbliche Amministrazioni che hanno necessità di collaborare l'una con l'altra in maniera interoperabile, efficiente e sicura sulla base di regole tecniche prestabilite.

Il modello è strutturato secondo il tipico "stack" del paradigma del cloud computing (i.e., livello infrastrutturale – IaaS; livello piattaforma - PaaS e livello applicativo - SaaS) dove l'enfasi, anche per i livelli infrastrutturali, viene posta appunto sul servizio e non più sul prodotto.

In generale, l'infrastruttura hardware e software è "multi-tenant" (ovvero in multi-proprietà) e condivisa tra più utenti; le risorse sono gestite in pool così da garantire risparmio e alta scalabilità anche a fronte di un più elevato numero di accessi ai servizi in rete. Esse, infatti, sono assegnate e riassegnate a seconda dell'effettiva domanda.

Ogni livello espone al livello soprastante un insieme di interfacce. Le interfacce sono aperte, possibilmente multicanale basate su standard, così da consentire un accesso ubiquo, unificato e affidabile ai servizi di ogni livello, nonché un forte riuso e interoperabilità. Il modello, e le interfacce di ogni livello, sono definiti attraverso specifiche regole tecniche e linee guida rilasciate dall'Agenzia per l'Italia Digitale, con un monitoraggio da parte dei suddetti organismi di governance dell'architettura sull'uso di tali interfacce, secondo le regole tecniche.

Il modello trova piena attuazione grazie al supporto di un insieme di servizi che agiscono a ogni livello. I servizi si distinguono in due macro-categorie: servizi di governance e coordinamento, servizi di sicurezza. L'insieme di tali servizi e i vari livelli del modello di cooperazione sono presentati nel dettaglio nelle seguenti sezioni.

E' bene rimarcare qui che mentre per lo "stack" mostrato in Figura 2 **l'Agenzia fornisce specifiche tecniche dettagliate di come le PA possono istanziare, a seconda delle proprie necessità e requisiti applicativi, tutti i livelli e i loro principali componenti, i servizi di supporto sono invece erogati da o per conto dell'Agenzia stessa al fine di consentire alle PA di dare piena operatività al modello e abilitare così l'interoperabilità tecnica, semantica e organizzativa.**

4.2.1. Livello infrastrutture (IaaS)

Il livello IaaS è suddiviso in due sottolivelli: il livello delle risorse computazionali e di storage, e il livello della rete. Il presente documento si focalizza in particolar modo sull'architettura di rete dispiegata nell'ambito dell'architettura IT di riferimento. Solo nella sezione 6, nel mostrare un esempio di istanziazione dell'architettura ad un caso di applicazione della Pubblica Amministrazione, si discute brevemente di un possibile modello di dispiegamento delle risorse computazionali (livello datacenter consolidation in Figura 2). Si rimanda i lettori interessati alle successive linee guida che l'Agenzia rilascerà in merito alla razionalizzazione dei centri di elaborazione dati delle Pubbliche Amministrazioni, così come già precedentemente evidenziato in sezione 2.1.3.

L'architettura di rete è un'architettura IP MPLS multiprovider, implementata attraverso lo strumento contrattuale dei contratti quadro multifornitore per i servizi di connettività o attraverso l'adesione di community network regionali secondo le previsioni del DPCM 1 aprile 2008 recante regole tecniche e di sicurezza SPC. L'insieme di tali soggetti ed eventuali ulteriori soggetti qualificati secondo le regole e le procedure previste dal CAD, sono collegati alla QXN. La QXN è il dominio di interconnessione degli operatori, costituito da un anello ridondato con due punti di ingresso uno su Roma e l'altro su Milano in corrispondenza dei NAP internet; tali punti di ingresso consentono l'interconnessione diretta tra gli operatori qualificati.
Il livello d'interconnessione e comunicazione tra le Amministrazioni è realizzato attraverso una componente di connettività che include servizi di trasporto per la trasmissione, secondo il protocollo IP, di dati, immagini e fonia, nonché servizi di interoperabilità di base, attraverso i quali viene attivata la trasmissione di informazioni o di documenti informatici. La condivisione, a livello nazionale, da parte delle Amministrazioni interconnesse di infrastrutture di connettività garantisce omogeneità ed uniformità di prestazioni da parte dei fornitori qualificati, consentendo lo sviluppo dell'SPC secondo un disegno unitario. L'architettura prevede l'esistenza di più ambiti omogenei che coinvolgono differenti soggetti:

1. un primo ambito denominato *intranet* e costituito dal dominio interno alla singola amministrazione che connette tutte le sedi della stessa distribuite sul territorio; è oggetto, per ogni amministrazione, di fornitura da parte di un unico fornitore.
2. un ambito di interconnessione denominato *infranet* che connette tra loro le singole amministrazioni o servite dallo stesso fornitore, oppure servite da fornitori diversi (in tale ultimo caso l'ambito di interconnessione è realizzato tramite la QXN);

3. un ambito denominato *internet* che consente l'interazione tra le singole amministrazioni e gli utenti esterni.

Tale architettura è stata pensata al fine di poter mettere a disposizione delle Pubbliche Amministrazioni servizi di trasporto con QoS garantita in modalità "end to end" nonché un livello adeguato di sicurezza.

4.2.2. Livello middleware (PaaS)

Il middleware di cooperazione è istanziato dalle Pubbliche Amministrazioni per consentire ad esse di interagire in maniera "seamless" e con garanzie di qualità ed efficacia, per il raggiungimento di obiettivi comuni e concordati reciprocamente, condividendo informazione attraverso i processi di business e lo scambio di dati tra i vari sistemi IT dispiegati.

Il middleware abilita diversi livelli di interoperabilità, così come definiti nell'ambito dell'European Interoperability Framework (EIF), i.e., interoperabilità organizzativa, interoperabilità semantica e interoperabilità tecnica. Esso è strutturato secondo lo "stack" protocollare del paradigma SOA in quanto, come in precedenza evidenziato, l'architettura è orientata ai servizi. Tale paradigma trova un ampio consolidamento di standard di mercato attraverso l'utilizzo delle tecnologie "Web Services".

Il punto di partenza è rappresentato dalla gestione dei processi (livello Process Management in Figura 2): le Pubbliche Amministrazioni che intendono aderire a SPC per fornire servizi applicativi integrati agli utenti finali definiscono i termini di un accordo dove indicare come e quando i loro singoli processi si interfacciano l'uno con l'altro. **In altre parole, per far in modo che diverse PA (organizzazione inter-PA), o diverse aree della stessa PA (organizzazione intra-PA), cooperino in maniera efficace, efficiente e sicura è necessario l'impiego di strumenti che consentano un allineamento e una gestione strutturata dei processi di business delle PA.** A tal fine, il modello proposto è sufficientemente generale e flessibile per abilitare strumenti di orchestrazione e di coreografia di servizi attraverso cui descrivere rigorosamente come il processo si struttura, quali flussi di controllo sono necessari, e come i messaggi vengono scambiati tra i servizi coinvolti nel processo.

L'interazione tra servizi avviene grazie all'esposizione di un contratto di servizio, ossia di un'interfaccia standard con viste di tipo: concettuale, logica e fisica che dettaglia come localizzare i servizi e quali funzionalità di business sono offerte dagli stessi, e come queste possono essere invocate. A tale contratto si aggiunge l'uso di metadati comuni e ontologie di riferimento per descrivere l'informazione che viene scambiata e annotazioni semantiche per dettagliare il modo in cui il servizio opera (i livelli Semantic e Service Description in Figura 2). **Si nota che il livello semantico consente di preservare e capire il significato dell'informazione durante l'interazione tra servizi di diverse Pubbliche Amministrazioni, e quindi di garantire interoperabilità semantica.**

Il middleware mette inoltre a disposizione i livelli tecnici necessari per la comunicazione. **A tal fine, l'architettura IT di riferimento supporta sia pattern di comunicazione basati sul paradigma request-response, sia pattern basati su paradigmi di pubblicazione e sottoscrizione di eventi (Messaging Services in** Figura 2**). Da ciò ne deriva che l'architettura consente la convergenza tra modelli di tipo SOA e modelli di tipo EDA.**

A tali livelli si aggiungono una serie di servizi abilitati dalle Pubbliche Amministrazioni "on-demand", dipendentemente dai requisiti del livello applicativo (livello SaaS). Così, i servizi di trasformazioni possono essere utilizzati qualora si debba far interagire servizi legacy che utilizzano formati e protocolli

di interscambio differenti, e i servizi di certificazione per certificare la congruità dei servizi applicativi dispiegati rispetto a stringenti requisiti di sicurezza/privacy o QoS in generale.

Le componenti della cooperazione applicativa (SPCoop), così come definite dalla norma, sono collocabili nel modello suddetto. Ad esempio, *l'accordo di servizio* è quella componente che include al suo interno le specifiche di processo (Process Management in Figura 2), così come tutti gli elementi tecnici necessari a descrivere l'interfaccia di ciascun servizio (Service Description in Figura 2); la *busta di e-GOV* definisce un formato comune di scambio request-response tra servizi applicativi delle pubbliche amministrazioni italiane (busta SOAP con estensioni – Messaging Service in Figura 2); la *porta di dominio* è quell'infrastruttura che implementa tutti i livelli tecnici di messaggistica (Secure Communication in Figura 2) e che può abilitare servizi di certificazione e trasformazione. **Tuttavia, il modello introdotto dal presente documento consente anche l'implementazione di altri scenari per l'interoperabilità: ad esempio, l'impiego di Web Services più leggeri di tipo restful e/o servizi ebXML. Ciò al fine di adattarsi alle diverse esigenze delle pubbliche amministrazioni, semplificando all'occorrenza anche l'uso dei suddetti elementi previsti dalla cooperazione applicativa.**

4.2.3. Livello applicativo (SaaS)

Il livello applicativo è rappresentato dai servizi applicativi (front office), tipicamente acceduti da utenti esterni al sistema SPC, e dai back office delle pubbliche amministrazioni. Rientrano in tale livello i sistemi informativi delle basi dati di interesse nazionale (authentic sources in Figura 2), servizi settoriali specifici (come ad esempio il fascicolo sanitario elettronico, servizi di gestione multe comunali, ecc.), portali web istituzionali e/o portali tematici.

L'Agenzia per l'Italia Digitale definisce le regole tecniche, per i servizi di tale livello, in merito agli standard di interoperabilità organizzativa, semantica e tecnica da adottare e alle caratteristiche di qualità tecniche e organizzative da garantire. Esse quindi includono le specifiche degli (i) aspetti organizzativi che i servizi applicativi devono rispettare per l'interazione con altri servizi applicativi all'interno di SPC; (ii) aspetti tecnici e semantici per garantire la corretta cooperazione e (iii) aspetti di usabilità, accessibilità, sicurezza dei servizi nell'interazione con l'utente finale.

I servizi del livello applicativo concorrono alla formazione dell'ecosistema dei servizi SPC solo se rispettano tutte le specifiche dettate dalle suddette regole tecniche. Gli organismi preposti alla governance di SPC hanno l'onere di monitorare il rispetto di tali regole mediante meccanismi di certificazione dei servizi.

4.2.4. Servizi di sicurezza

Dal punto di vista della sicurezza, l'intero livello infrastrutturale si configura come un dominio affidabile (trusted), costituito a sua volta da una federazione di domini affidabili basata su mutue relazioni organizzative e tecnologiche di tipo fiduciario.
In tale scenario, è importante notare che la sicurezza è un elemento trasversale alle componenti di connettività e cooperazione; esso include l'insieme delle misure organizzative, dei servizi e delle infrastrutture realizzate a livello centrale (dominio di interconnessione) e a livello di singola

Amministrazione (dominio interno), in conformità alle regole tecniche definite in ambito DPCM 1 aprile 2008.
Data l'architettura distribuita del sistema, l'organizzazione per la sicurezza è realizzata con strutture che operano in ciascun dominio, ma interconnesse e coordinate in modo da costituire virtualmente un'unica struttura operativa. I compiti di armonizzazione, indirizzo generale e coordinamento sono assolti a livello centrale, le funzioni di gestione e monitoraggio sono assolte a livello locale.
Per garantire la sicurezza del SPC sono definite regole e requisiti minimi di sicurezza, concordati tra i vari soggetti, che vengono, pertanto, applicati su tutte le reti collegate e in tutte le loro componenti.
Questo porta alla necessità di:

1. individuare i soggetti coinvolti nella gestione della sicurezza (centrali e locali);
2. definire le responsabilità, i confini e l'ambito di azione di ciascuno;
3. definire e stabilire le misure minime di sicurezza e le loro modalità di applicazione.

L'erogazione dei servizi di sicurezza da parte di ciascun fornitore qualificato avviene mediante uno o più Centri Operativi per la sicurezza, Security Operating Center (SOC).
Nell'ambito dei servizi di sicurezza di cui sopra è stato individuato l'insieme di servizi di base ovvero l'insieme di servizi di cui ogni amministrazione nel SPC deve obbligatoriamente dotarsi per garantire il livello minimo di sicurezza previsto;
I servizi base variano in funzione della tipologia di rete con cui il singolo dominio di un'amministrazione è interconnesso. Le tipologie di rete previste in SPC si suddividono in:

- **Reti fidate** (*trusted*), con cui si individua qualsiasi rete messa a disposizione da un fornitore SPC, impiegata da una pubblica amministrazione per interconnettersi ad un'altra pubblica amministrazione. In tal senso le infrastrutture di rete di un fornitore SPC ed la rete QXN costituiscono reti fidate.
- **Reti non fidate** (*untrusted*), con cui si individua qualsiasi rete che non faccia parte del SPC ed interconnessa a quella di una pubblica amministrazione. In tal senso la rete Internet o qualsiasi altra rete non appartenente all'SPC interconnessa con una pubblica amministrazione costituiscono reti non fidate.

Per quanto concerne invece la sicurezza finalizzata all'accesso dei servizi applicativi e telematici, allo scopo di garantire l'aggiornamento, la veridicità e l'affidabilità dell'intero insieme di informazioni che possono essere scambiate nell'interazione tra diverse PA, sono assicurati, in particolare: il riconoscimento dei soggetti abilitati ad operare in SPC e delle componenti del middleware di cooperazione e del livello applicativo (e.g., porte di dominio, servizi applicativi), nonché la gestione delle identità digitali e dei ruoli su base federale.
In quest'ultimo caso, il modello adottato è il modello GFID [5] che si basa sul principio di creare un livello di astrazione che mascheri l'eterogeneità di eventuali sistemi già esistenti per la gestione delle identità. In pratica, con tale modello le pubbliche amministrazioni e le aziende condividono le informazioni sulle identità mantenendo invariate le proprie soluzioni di gestione degli account degli utenti e di accesso ai servizi applicativi. Il modello consente di attestare sia le identità di un utente, sia il suo ruolo (ossia un insieme di attributi che individua lo specifico compito dell'utente all'interno della pubblica amministrazione). Le entità responsabili di validare l'identità, il ruolo e altri attributi specifici di un utente sono gli Identity Provider e le Attribute Authority rispettivamente.

Si rimarca che il modello presentato in [5] è un modello già istanziabile nell'architettura IT di riferimento per una gestione sistemica e unitaria delle identità digitali; esso quindi può essere utilizzato nel supportare le funzionalità richieste dall'adozione del documento digitale unico introdotto dal DL n.179/2012. Al momento manca una classificazione che consenta alle PA di definire i livelli sicurezza necessari per l'accesso ai servizi; tale modello riprendendo esperienze internazionali, in alcune delle quali l'Agenzia è coinvolta, verrà prossimamente definito anche sulla base della nuova versione di linee guida "per la stesura di convenzioni per la fruibilità di dati delle pubbliche amministrazioni convenzioni per l'utilizzo di banche dati accessibili in rete" per le quali è appena pervenuto il parere positivo del Garante della Privacy.

4.2.5. Servizi di governance e coordinamento

Come detto in precedenza, a supporto del modello di cooperazione per l'interoperabilità introdotto nel presente documento, è necessario fornire un insieme di servizi nazionali che complementano gli elementi del middleware di cooperazione nel garantire i diversi livelli di interoperabilità. Essi rappresentano, quindi, quei mattoni di base per assicurare la piena interoperabilità dei sistemi IT delle PA connessi a SPC. Tali servizi possono essere classificati in servizi di supporto all'interoperabilità semantica, organizzativa e tecnica.

Per l'interoperabilità semantica, rientrano tra i servizi di supporto nazionali i cosiddetti asset semantici, per usare la terminologia utilizzata in ambito europeo nel contesto del programma ISA. Per asset semantici si intendono schemi comuni di dati, ontologie comuni per diversi settori (quelli che in ambito europeo sono detti "core vocabularies" [14], e.g., Core Person, Core Location, Core Public Service), classificazioni nazionali (e.g., classificazione ATECO, classificazione S-13 delle pubbliche amministrazioni), tesauri e dataset di riferimento, cataloghi nazionali (e.g., il Repertorio Nazionale dei Dati Territoriale [15], gestito dall'Agenzia per l'Italia Digitale che include i metadati dei dati territoriali delle pubbliche amministrazioni, può essere considerato nello specifico contesto dei dati geospaziali un asset semantico), nonché l'insieme dei riferimenti a ontologie e standard tecnici per la descrizione di dati anche settoriali (e.g., dati sanitari, dati culturali).

Le linee guida per la valorizzazione del patrimonio informativo pubblico prima menzionate, e relative all'anno 2013, includono già una prima lista di tali riferimenti e possono quindi essere utilizzate come asset dalle pubbliche amministrazioni per individuare gli standard tecnici e le ontologie necessarie alla descrizione dei propri dati (anche quelli relativi alle basi di dati di interesse nazionale).

Per l'interoperabilità organizzativa e tecnica, i servizi di supporto nazionali includono i registri necessari a "localizzare" i servizi resi disponibili dalle pubbliche amministrazioni all'interno del perimetro SPC e gli indici di riferimento nazionali. Così, rientrano in tale categoria, i registri utilizzati per individuare le entità abilitate dal modello GFID (i.e., AR – Authority Registry per identificare l'Identity Provider di riferimento per validare l'identità di un utente, AAR – Attribute Authority Registry per identificare l'Attribute Authority di riferimento per validare il ruolo di un utente), i registri per scoprire i servizi applicativi e i processi di cooperazione delle PA disponibili nel sistema SPC (e.g., registro SICA, registro delle convenzioni) e gli indici nazionali per individuare univocamente le pubbliche amministrazioni italiane (i.e., IPA) e i gestori PEC (i.e., IGPEC).

Si noti che ognuno di tali servizi è realizzato sulla base di un'architettura di riferimento propria ben definita. Lo scopo di tale documento tuttavia non è quello di descrivere nel dettaglio tali architetture ma di presentare il modello generale dell'architettura IT di riferimento della PA italiana, istanziandolo in un caso concreto. Si rimanda pertanto alle linee guida più specifiche per una descrizione puntuale di come ogni servizio prima introdotto interagisce con quelli del middleware di cooperazione al fine di garantire piena interoperabilità.

In aggiunta a tali servizi di supporto, i servizi di governance e coordinamento includono servizi di gestione del sistema (e.g., trouble ticketing, servizi di monitoraggio) e servizi di coordinamento della sicurezza, i.e., CERT.
Per quanto riguarda quest'ultimo caso, alla luce delle nuove previsioni normative in materia di sicurezza cibernetica, l'Agenzia è allo stato impegnata a definire l'architettura di riferimento per il CERT della PA. In tale ambito sono in via di definizione regole, organizzazione e meccanismi applicabili nell'ambito della intera Pubblica Amministrazione italiana. Tale struttura è inserita nello scenario delineato dal DPCM 24 gennaio 2013 sulla sicurezza cibernetica, che vede l'Agenzia quale parte attiva nella gestione della sicurezza della Pubblica Amministrazione Italiana.
La Commissione di Coordinamento SPC svolge attività di indirizzo operativo e controllo sull'intero sistema, facendo in modo che vengano assicurati i livelli di sicurezza stabiliti mediante la figura di un Responsabile della Sicurezza SPC a cui riferisce il Responsabile operativo della Sicurezza SPC del Centro di Gestione della Sicurezza SPC.
Il CERT della PA rappresenta pertanto l'organo referente centrale per la prevenzione, il monitoraggio, la gestione e il follow-up degli incidenti di sicurezza, assicurando l'applicazione di metodologie coerenti e uniformi in tutto il sistema. Esso non si sostituisce alle funzioni organizzative degli altri soggetti SPC, ma collabora attivamente con essi, secondo le modalità stabilite d'intesa con la Commissione di Coordinamento SPC. Il CERT può inoltre assumere, almeno in parte, un ruolo nella gestione e risoluzione degli incidenti di sicurezza.
Lo scenario definito prevede che in ogni amministrazione, presso ciascun operatore e presso la QXN sia costituita una struttura organizzativa denominata Unità locale di Sicurezza SPC, per la gestione degli aspetti relativi alla sicurezza.
Tali Unità locali, che costituiscono la parte distribuita del sistema di sicurezza SPC, sono ognuna coordinata da un Responsabile operativo locale della Sicurezza SPC che rappresenta l'interfaccia verso le altre strutture organizzative che compongono il sistema di sicurezza del SPC.

5. MODELLI DI DEPLOYMENT DI MERCATO

Il deployment tecnico delle architetture nei differenti casi d'uso, in particolare per il livello di "cooperation middleware" (Figura 2), deve essere definito in funzione delle variabili locali proprie del contesto specifico di applicazione, ad esempio per quanto concerne il sistema informativo relativo all'ANPR vanno tenuti in conto il pregresso, gli attori, i servizi specifici da garantire, i dati quantitativi dei processi , etc.. Un dominio come l'ANPR può considerarsi un dominio di business, che implementa l'architettura IT nazionale utilizzandone modelli, linee guida e servizi per l'interoperabilità, allo scopo di garantire un modello documentato ed interoperabile non solo al suo interno ma con altri domini come a titolo di esempio la Sanità con il fascicolo sanitario elettronico.

Il capitolo presente è dedicato ai "modelli di deployment di mercato" che rappresentano le modalità di ingaggio tra pubbliche amministrazioni e fornitori. Tali scenari possono essere perseguiti anche in maniera combinata.

Mentre le architetture le linee guida e gli standard hanno lo scopo di standardizzare la domanda e creare condizioni di interoperabilità, che consentano uno sviluppo armonico delle soluzioni tecniche, gli scenari di deployment di mercato devono organizzare l'offerta. Entrambi gli approcci verso la domanda e verso l'offerta, a maggior ragione se perseguiti in modo coordinato, rappresentano sia elementi di governance per lo sviluppo dell'agenda digitale Italiana sia, in via più generale, elementi di politica industriale del settore ICT.

I modelli di deployment di mercato che possono essere individuati sono: self-managed, attraverso offerte di fornitori qualificati, attraverso centrali di committenza e attraverso centri servizio PA. Essi sono brevemente introdotti nel seguito.

5.1. Deployment self-managed

Sulla base delle linee guida, delle regole tecniche (ove presenti), degli standard individuati e seguendo le architetture di riferimento, con i relativi modelli di interconnessione e le interfacce ove definite, le Amministrazioni, in via autonoma, realizzando direttamente le soluzioni tecniche o in qualità di stazioni appaltanti, possono definire le proprie procedure di procurement controllando il rispetto dei requisiti tecnici ed architetturali nonché degli standard adottati. Tale approccio può essere consigliato quando l'ambito è sufficientemente ampio, caratterizzato da specificità, da un pregresso, laddove sono presenti capacità tecniche, organizzative e manageriali di tipo tecnico. E' una modalità rischiosa quando sono assenti i presupposti indicati, specialmente in assenza di elenchi di fornitori qualificati o a seconda dei casi di soluzioni a catalogo.

5.2. Deployment attraverso offerte di fornitori qualificati

L'Agenzia potrebbe direttamente, ma meglio indirettamente attraverso l'abilitazione di specifiche "accreditation authorities", qualificare fornitori privati (e pubblici) per categorie di servizi. Tali processi potrebbero caratterizzarsi da una qualunque combinazione di: "garanzie ai morsetti"; certificazioni; impegni al rispetto di standard, linee guida e criteri di interoperabilità; livelli di sicurezza, etc.. Le specifiche soluzioni o linee di offerta potrebbero, inoltre, essere soggette a certificazione

documentale e tecnica per comprovarne rispetto di standard, di modello di architettura di requisiti tecnici, di interoperabilità e di sicurezza. Tale modalità avrebbe il pregio di favorire un'offerta qualificata e standardizzata e favorire l'introduzione di soluzioni e modelli innovativi. Calibrando i processi di qualificazione, ad esempio enfatizzando alcune modalità si possono determinare o favorire sviluppi in talune direzioni. Per esempio enfatizzando le "garanzie ai morsetti" si può favorire la *commoditization* e quindi un più facile e competitivo accesso a prodotti/servizi. Oppure enfatizzando gli aspetti di interoperabilità si possono favorire la federabilità di soluzioni. I due precedenti esempi si calzano perfettamente nel caso rispettivamente delle soluzioni cloud computing o nello sviluppo di sistemi di gestione di identità digitali. La possibilità descritta nel presente paragrafo avrebbe anche il supporto normativo del CAD, che all' art. 82 prevede "*la costituzione di elenchi di fornitori qualificati a livello nazionale e regionale per la realizzazione delle finalità SPC*" (gli ambiti generali riguardano i servizi di rete, applicativi e di sicurezza)[1]. I fornitori iscritti negli elenchi supererebbero la fase di prequalifica nelle gare a procedura ristretta a livello nazionale, non escludendo tuttavia che atri soggetti pur non presenti nei predetti elenchi possano qualificarsi in sede di procedura di gara. Tale modello favorirebbe la possibilità, indipendentemente dall'avere acquisito un contratto, di essere on line e pronti per l'erogazione di servizi alle PA.

5.3. Deployment attraverso centrali di committenza

Centrali di committenza dotate di capacità tecniche e di dimensioni adeguate possono definire ambiti di fornitura conformi degli standard individuati, seguendo inoltre le architetture di riferimento ed i relativi modelli di interconnessione e interfaccia. Il procurement attraverso tali procedure garantirebbe le stazioni appaltanti (PA) dotate di minori competenze e conoscenze, potendosi porre in capo a tali centrali il controllo dei requisiti tecnici ed architetturali ed il rispetto degli standard.

5.4. Deployment attraverso centri servizio PA

Centri di servizio tematici o pluritematici potrebbero essere qualificati per fornire ospitalità ad applicazioni di diverse PA aggregate su base geografica o tematica, favorendo un consolidamento e razionalizzazione dei datacenter delle PA. Tali centri servizi dovrebbero fornire garanzie di risparmio energetico, altissima affidabilità prestazionale, interconnessione di rete con ampia banda e ridondanza, caratteristiche di sicurezza fisica e logica elevate. Lo stesso modello potrebbe essere utilizzato per tematiche applicative specifiche, che per loro natura è preferibile che siano in mano pubblica quali ad esempio: hub per pagamenti ed incassi delle PA, servizi per ASL, banche dati di interesse nazionale.

[1] Lo schema di decreto che consentirebbe l'avvio di tale modalità è stato licenziato dalla Commissione di coordinamento SPC ed a settembre del 2011 inviato dall'allora DigitPa all'ufficio legislativo dell'allora Ministero vigilante. Il relativo provvedimento non è stato emanato.

6. CASO DI STUDIO: L'ANAGRAFE DELLA POPOLAZIONE RESIDENTE

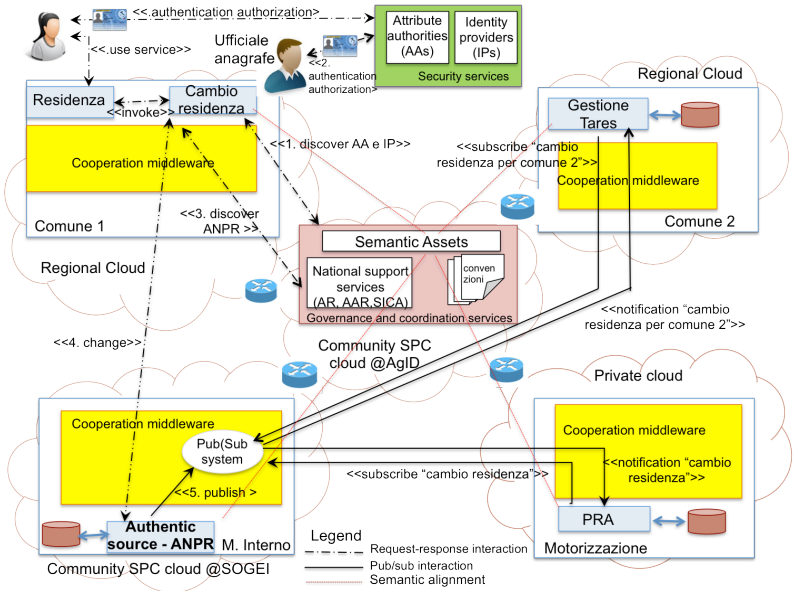

Figura 3: L'applicazione del modello di cooperazione al caso dell'ANPR

Tutte le componenti dell'architettura IT di riferimento possono essere utilizzate convenientemente per implementare la nuova l'Anagrafe della Popolazione Residente (ANPR).

L'ANPR è stata recentemente rivista nel suo modello dal DL n. 179/2012 al fine di superare alcune problematiche emerse nella gestione, fin ad ora messa in pratica, dei dati anagrafici (e.g., mancanza di dati aggiornati a livello centrale, inutile duplicazione di dati, per citarne alcune). Il modello che prevede il dispiegamento di anagrafi locali presso i comuni con un coordinamento centrale del Ministero dell'Interno attraverso un insieme di indici, è stato quindi sostituito da un modello in cui viene creata un'anagrafica unica nazionale gestita interamente dal Ministero dell'Interno presso SOGEI. I comuni, e tutte le altre amministrazioni interessate a dati di tipo anagrafico, interrogano la base di dati centrale del Ministero dell'Interno per poter accedere in maniera "seamless" ai dati anagrafici della popolazione ed erogare così servizi applicativi ai propri utenti finali (e.g., cambio di residenza in tempo reale, aggiornamento del pubblico registro automobilistico, ecc.).

I dati anagrafici dell'ANPR sono, tra gli altri, nome, cognome, codice fiscale, indirizzo, domicilio digitale e altre informazioni sullo stato di famiglia di ogni cittadino sia italiano, sia straniero residente nel nostro paese.

Alla luce di tale scenario si evince che il successo dell'ANPR dipende fortemente dall'abilità delle PA di interagire in maniera interoperabile, rispettando allo stesso tempo requisiti di qualità, sicurezza e privacy

e da un opportuno dimensionamento del sistema che deve saper rispondere dinamicamente a un elevato numero di richieste di accesso, anche simultanee, da parte di diversi sistemi.

La Figura 3 mostra come le componenti dell'architettura SPC possano essere utilizzati per la realizzazione dell'ANPR. In particolare, per semplicità, la figura evidenzia solo un sottoinsieme limitato di operazioni che la base di dati di interesse nazionale deve supportare. L'esempio illustra il caso di un cittadino che vuole effettuare un cambio di residenza online dal Comune 2 al Comune 1.

Il cittadino accede al servizio di residenza del Comune 1 previa autenticazione attraverso il Documento Digitale Unificato. L'autenticazione è gestita secondo il modello GFID utilizzato in SPC che prevede la validazione delle credenziali presso un Identity Provider. Il cittadino così autenticato riesce ad accedere al front-end web del servizio di cambio residenza e a iniziare l'operazione di inserimento dei propri dati per effettuare il cambio residenza. Tali interazioni attivano il servizio relativo del Comune 1. La pratica è gestita da un ufficiale dell'anagrafe, l'unico titolato a poterla gestire. A tal riguardo anche l'ufficiale si autentica al sistema: attraverso i registri nazionali di supporto per il modello GFID (i.e., AR, e AAR), le sue credenziali e il suo ruolo sono validati da un Identity Provider e un Attribute Authority consentendogli così di avviare l'intera pratica.

La pratica si espleta attraverso un insieme di interazioni intra-PA regolate da specifiche convenzioni. Tecnicamente, le interazioni sono sia di tipo request-response (e.g., si richiede di poter accedere a una funzionalità specifica del servizio ANPR) sia di tipo publish-subscribe (e.g., alcuni attori si sottoscrivono a un evento di interesse al verificarsi del quale vengono notificati per consentirgli poi di compiere sui propri sistemi un insieme di azioni).

Nell'esempio, il servizio di back office del Comune 1 definisce il processo di interazione con l'ANPR per la comunicazione di nuovi dati di residenza. Sulla base di tale processo, opportunamente descritto mediante le funzionalità offerte dal Process Management del Cooperation middleware, viene effettuata una chiamata a un servizio di "cambio dati di residenza" messo a disposizione dall'ANPR e individuato grazie all'ausilio dei registri nazionali (i.e., registro SICA). Tale chiamata può essere sincrona e gestita dai livelli semantici e tecnici del middleware di cooperazione. In particolare, si fa uso di asset semantici, come prima discusso, per descrivere i dati coinvolti nell'interazione (a mero titolo d'esempio, Core Person [16] e/o FOAF – Friend of A Friend [17] possono essere utilizzati per descrivere i dettagli delle persone e Core Location [18] per descrivere quelli relativi agli indirizzi delle residenze).

Il servizio dell'ANPR invocato agisce opportunamente sulla base di dati e notifica, attraverso un sistema publish/subscribe dispiegato presso il Ministero dell'Interno, che un cambio di residenza dal Comune 2 al Comune 1 si è verificato. Il Comune 2, così come altri attori che possono essere coinvolti nel processo (in Figura 3 la motorizzazione è interessata ad aggiornare i dati della residenza della persona nel proprio registro pubblico automobilistico) e sottoscritti all'evento del cambio di residenza, sono notificati e provvedono ad agire sulle proprie applicazioni locali per aggiornare i dati in tempo reale.

Per quel che riguarda il dispiegamento delle risorse, la Figura 3 mostra un modello di cloud ibrido dove diverse cloud di comunità SPC (ivi incluse le cloud regionali che possono essere create al fine di ospitare i servizi dei comuni localizzati nella regione) interagiscono con cloud privati di alcune pubbliche amministrazioni.

Infine, si ritiene che nel caso di studio presentato dell'ANPR, la fase di consolidamento deve utilizzare il modello 4 "centri servizio PA", avviando l'attivazione del modello 2 per qualificare i fornitori di

software di gestione comunali, ovvero del modello "self managed" per i grandi comuni.

7. BIBLIOGRAFIA

[1] EUROPA 2020 - Una strategia per una crescita intelligente, sostenibile e inclusiva - COM(2010) 2020.

[2] Agenda Digitale Europea, http://ec.europa.eu/information_society/digital-agenda/index_en.htm, 2013

[3] European Commission, New Digital Priorities for 2013-2014, http://europa.eu/rapid/press-release_IP-12-1389_en.htm, 2013

[4] Agenda Digitale Italiana, http://www.agenda-digitale.it/agenda_digitale/, 2013

[5] Agenzia per l'Italia Digitale, "Modello di gestione federata delle identità digitali (GFID)", http://www.digitpa.gov.it/sites/default/files/allegati_tec/SPCoop-ModelloGFID_V1.5.1.pdf, 2011

[6] Commissione di Coordinamento SPC, "Linee guida per l'interoperabilità semantica attraverso i Linked Open Data", http://www.digitpa.gov.it/sites/default/files/allegati_tec/CdC-SPC-GdL6-InteroperabilitaSemOpenData_v2.0_0.pdf , 2012

[7] Agenzia per l'Italia Digitale, "Architettura per le Comunità Intelligenti: Visione Concettuale e Raccomandazioni alla Pubblica Amministrazione, http://www.digitpa.gov.it/sites/default/files/ArchSC_v2.0.pdf, 2012

[8] Commissione di Coordinamento SPC, "Definizione dei contenuti delle gare S2 S3", http://www.digitpa.gov.it/sites/default/files/allegati_tec/CdC-SPC-GdL4-ContenutiGareS2S3-v1%200.pdf, 2012

[9] Commissione di Coordinamento SPC, "Definizione dei requisiti tecnici per la transizione, l'evoluzione e il funzionamento delle Infrastrutture Condivise", http://www.digitpa.gov.it/sites/default/files/allegati_tec/CdC-SPC-GdL6-InfrastruttureNazionaliCondivise-v1.5_0_0.pdf, 2012

[10] Commissione Europea, Comunicazione della Commissione al Parlamento Europeo, al consiglio, al comitato economico e sociale europeo e al comitato delle regioni – Un'agenda digitale europea, 2010

[11] Cassa Depositi e Prestiti – Studio di settore, "Banda larga e Reti di Nuova Generazione – La banda larga in Italia: presupposti per lo sviluppo di un'infrastruttura strategica", Agosto 2012.

[12] IStat – Report,"Cittadini e nuove tecnologie", 20 dicembre 2011, http://www.istat.it/it/files/2011/12/ICT-famiglie-2011.pdf?title=Cittadini+e+nuove+tecnologie+-+20%2Fdic%2F2011+-+Testo+integrale.pdf

[13] ISO/IEC 25012 "Data Quality Model". 2008.

[14]European Commission, "e-Government Core Vocabularies",

https://joinup.ec.europa.eu/community/core_vocabularies/description, 2013.

[15] Agenzia per l'Italia Digitale, "Repertorio nazionale per i dati territoriali – RNDT", http://www.rndt.gov.it/RNDT/home/index.php, 2013

[16] European Commission, Core Person Vocabulary http://joinup.ec.europa.eu/asset/core_person/description, 2013.

[17] FOAF Vocabulary Specification, http://xmlns.com/foaf/spec/, 2013.

[18] European Commission, Core Location Vocabulary https://joinup.ec.europa.eu/asset/core_location/description, 2013.