Il motore di ricerca delle offerte contraffatte online potrà essere utilizzato dall'UIBM sia per finalità di studio e analisi del fenomeno sia - su delega da parte dei titolari dei diritti di proprietà industriale - per il monitoraggio di brand e prodotti sulle piattaforme/*merchant* aderenti a *Carta Italia*.

Attività 2016

Nel corso del 2016 sono state svolte le seguenti attività:

- analisi del processo *Carta Italia*, volta alla formalizzazione tecnica del protocollo di intesa;
- analisi di sicurezza del sistema, volta all'individuazione dei requisiti tecnici di progettazione;
- realizzazione del primo prototipo del sistema di monitoraggio delle offerte contraffatte sulle piattaforme/*merchant* aderenti a *Carta Italia*;
- progettazione di un sistema di gestione delle segnalazioni di violazione dei diritti di proprietà industriale;
- sviluppo di uno strumento automatico di rilevamento di siti potenzialmente contraffattori.

DELIVERABLE

- "Analisi di processo *Carta Italia*";
- "Definizione dei requisiti utente del sistema di gestione delle segnalazioni";
- "Processo di segnalazione e caso d'uso per invio segnalazione";
- "Requisiti del prototipo di ricerca dei brand contraffatti online".

SICUREZZA E PRIVACY

UIBM-ATA

Analisi Tecnologie Anti-contraffazione

Progetto in convenzione con MiSE DGLC-UIBM

Realizzazione di un sistema informatico per la sottomissione verso l'UIBM delle tecnologie dei prodotti anticontraffazione offerti sul mercato e di un sito-vetrina con la presentazione delle tecnologie.

Obiettivi

Il Progetto ha lo scopo di realizzare un sistema per la sottomissione dei prodotti anticontraffazione da parte dei produttori verso l'UIBM e di offrire un servizio di orientamento alle aziende sulle tecnologie anticontraffazione in base al settore di applicazione.

Impatto

Il servizio online di presentazione delle tecnologie anticontraffazione alle aziende - basato sulla raccolta e categorizzazione delle tecnologie - faciliterà la comprensione dei campi di applicazione e dei limiti di utilizzo delle diverse tecnologie disponibili.

Per ogni tecnologia saranno riportate le principali caratteristiche tecniche e i settori di utilizzo, in modo che le imprese possano ottenere informazioni circa la tecnologia più adatta alle proprie esigenze.

Descrizione

Nello specifico le attività del Progetto possono essere descritte come segue.

Formalizzazione del processo di sottomissione dei prodotti anticontraffazione

L'attività ha lo scopo di formalizzare il processo di sottomissione/aggiornamento/eliminazione dei prodotti anticontraffazione da parte dei produttori verso l'UIBM. L'analisi del processo tiene in considerazione anche gli aspetti di sicurezza informatica, al fine di mitigare possibili rischi connessi alla sottomissione di prodotti anticontraffazione.

Formalizzazione del processo di presentazione delle tecnologie anticontraffazione

L'attività ha lo scopo di formalizzare il processo di presentazione al pubblico delle tecnologie anticontraffazione. Il sistema è basato su due livelli:

a) al primo livello sono presentate le classi di tecnologie anticontraffazione;

b) al secondo livello, collegato al primo, possono essere visualizzate le specifiche tecnologie di ogni classe.

Nell'analisi del processo sono tenuti in considerazione anche gli aspetti di sicurezza informatica, al fine di mitigare possibili rischi connessi all'offerta del servizio di presentazione delle tecnologie anticontraffazione.

Sistema di sottomissione dei prodotti anticontraffazione

Il sistema di sottomissione dei prodotti anticontraffazione è progettato al fine di classificare il prodotto sottomesso secondo determinati criteri, come ad esempio la tecnologia utilizzata e il settore di riferimento.

La sottomissione di prodotti anticontraffazione è accessibile a tutti i produttori del settore.

Sistema di presentazione delle tecnologie anticontraffazione

Il servizio rappresenta il punto di riferimento informativo per orientare le aziende sull'uso delle tecnologie anticontraffazione disponibili. La presentazione delle tecnologie è effettuata anche sulla base delle informazioni fornite dal produttore, classificando i prodotti in base alla tecnologia utilizzata e al settore di riferimento.

Attività 2016

Nel corso del 2016 sono state svolte le seguenti attività:

- analisi del processo di sottomissione, aggiornamento e rimozione dei prodotti anticontraffazione da parte dei produttori;
- analisi di sicurezza;
- analisi dei requisiti di progettazione del sistema informatico di sottomissione/aggiornamento/rimozione delle tecnologie anticontraffazione e della vetrina online;
- realizzazione della prima versione del modulo di presentazione delle tecnologie anticontraffazione;
- realizzazione della prima versione della pagina web di presentazione del servizio;
- realizzazione della prima versione del sistema automatico di gestione (comprensivo dei messaggi per l'utente relativi all'avanzamento del processo).

DELIVERABLE

- "Processo di sottomissione dei prodotti anticontraffazione".
- "Requisiti del sistema informatico di sottomissione delle tecnologie anticontraffazione e della vetrina online".

SICUREZZA E PRIVACY

OCTAVE

Objective Control of TAlker VErification

Progetto nel Programma Horizon 2020 della Commissione europea

Il Progetto "OCTAVE", che s'inquadra nel settore "Secure Societies" del Programma Horizon 2020, coinvolge dodici partner di sette Stati Membri (Italia, Danimarca, Finlandia, Francia, Grecia, Regno Unito, Spagna) organizzati in un consorzio che vede la partecipazione bilanciata di partner industriali e accademici. Il Progetto intende superare la complessità dell'utilizzo e della gestione di password testuali per il controllo di accesso logico a sistemi informatici, e il controllo di accesso fisico ad aree critiche.

Obiettivi

OCTAVE ha l'obiettivo di realizzare un sistema di verifica dell'identità di un utente attraverso la sua voce, con innovative soluzioni tecnologiche e di piattaforma operativa che concorrono a un riconoscimento più affidabile rispetto a quello consentito dagli attuali metodi di verifica del parlante. Per essere utilizzabile in modo indipendente da una molteplicità di fornitori di applicazioni e servizi, il sistema verrà realizzato su piattaforma cloud, con avanzati accorgimenti di sicurezza.

Impatto

L'industria e le attività produttive necessitano di alternative all'utilizzo di password testuali o token (chiavette, smartcard, ecc.), che possono essere rubati o trasferiti ad altre persone. Una tecnologia biometrica fornisce soluzioni affidabili, efficaci, contenute nei costi e facili da usare. In particolare, la biometria vocale fornisce sistemi automatici di verifica dell'identità del parlatore utilizzabili con una varietà di dispositivi di accesso, tra cui anche smartphone e tablet. Sistemi biometrici alternativi come il riconoscimento dell'iride, le impronte digitali o il riconoscimento facciale sono considerati meno accettabili dagli utenti rispetto al riconoscimento tramite la voce, che richiede soltanto di parlare a un microfono. Il sistema di autenticazione biometrica TBAS (Trusted Biometric Authentication System) consentirà di:

- decifrare correttamente l'impronta vocale anche in luoghi rumorosi (environmental robustness);
- impedire l'accesso ad aree sensibili a persone non autorizzate, anche in assenza di specifica sorveglianza degli ingressi;
- assicurare l'affidabilità e la privacy, tramite tecniche di riconoscimento rapide ed efficaci che permettano di prevenire, ad esempio, tentativi di contraffazione della voce dell'utente legittimo.

Descrizione

Il Progetto parte dalle tecnologie esistenti che hanno già una loro maturità commerciale. Il prodotto commerciale della società ValidSoft, con sede in Gran Bretagna e filiali in vari altri Paesi, è la baseline per un sistema ancora più avanzato che OCTAVE svilupperà focalizzandosi sulla soluzione di alcuni problemi che limitano le prestazioni dei sistemi attuali.

OCTAVE prevede una sperimentazione in due applicazioni: l'accesso a servizi online di Findomestic,

società finanziaria del gruppo bancario BNP Paribas, e l'accesso a infrastrutture critiche dell'Aeroporto di Linate. Le valutazioni effettuate in contesti reali su servizi critici legati ai servizi bancari e agli accessi controllati in strutture "sensibili" come quelle di un aeroporto, permetteranno di verificare e dimostrare la flessibilità del sistema e la sua utilizzabilità anche in altri contesti commerciali.

La presenza nel Progetto di dipartimenti universitari e istituti di ricerca molto reputati nel contesto delle tecnologie di trattamento della voce (University of Herdfordshire in Gran Bretagna, University of Eastern Finland, Aalborg University in Danimarca, Eurecom in Francia, e la stessa FUB) e nel contesto delle tecniche di sicurezza ICT (ancora FUB e l'istituto greco AIT) garantirà la selezione e la messa a punto degli algoritmi più avanzati per la realizzazione di componenti da integrare nel sistema baseline di ValidSoft o in altri sistemi di tipo open source, o di terze parti. La soluzione proposta dal Progetto, infatti, si presta ad essere innestata su qualsiasi sistema che esponga opportune API (Application Programming Interfaces).

Il coinvolgimento degli utenti avviene in due fasi, la prima una tantum, la seconda ad ogni utilizzo del sistema:

- fase di arruolamento (enrolment), finalizzata all'iscrizione di un utente in una lista (database) di utenti autorizzati e alla memorizzazione dell'impronta biometrica vocale associata a quell'utente;
- fase di esercizio, nell'ambito della quale ogni utente che si presenti per l'accesso (fisico o logico) rilascia un campione di voce, da cui viene estratta un'impronta vocale che viene confrontata con l'impronta conservata nel database, al fine di poter verificare l'identità dell'utente come autentica e abilitarlo ad accedere a specifici servizi online o aree fisiche riservate nell'ambito dell'aeroporto di Linate.

Attività FUB 2016

Coordinamento. La Fondazione ricopre il ruolo di ente Coordinatore della realizzazione del Progetto, secondo le linee guida di un Project Management Handbook realizzato a inizio Progetto. Un aspetto rilevante dell'attività di coordinamento consiste nel presidiare il processo di integrazione delle componenti tecnologiche sulla piattaforma, al fine di garantire che l'integrazione avvenga in aderenza agli obiettivi del Progetto e nel rispetto delle esigenze di ogni partner, in termini di diritti di proprietà intellettuale e valorizzazione economica dei risultati prodotti da ognuno.

Nel 2016 la Fondazione ha coordinato tre riunioni plenarie di progetto (14-16 marzo, Atene; 28 ottobre, Roma; 21-23 novembre, Londra), due riunioni di coordinamento a mezzo video-conferenza e numerose riunioni tecniche, di workpackage o bilaterali tra workpackage o tra Partner, tutte in video-conferenza. OCTAVE ha superato con successo la prima riunione di verifica tecnica (Bruxelles, 12 luglio 2016) da parte del competente Ufficio Progetti della Commissione Europea. Nel corso della verifica, la Fondazione ha ottenuto un'esplicita nota elogiativa per la sua opera di coordinamento.

Contribuzione tecnico-scientifica. La Fondazione conduce il gruppo di lavoro (workpackage 7), dedicato alla progettazione e realizzazione delle prove di laboratorio e alla supervisione scientifica dello svolgimento delle prove in campo. La progettazione delle prove comprende la disamina di numerosi corpora vocali, al fine di costituire un "super dataset" per le specifiche necessità di test del Progetto. Le prove di laboratorio saranno effettuate da FUB, con il supporto degli altri partner accademici, e forniranno indicazioni sulle prestazioni ottenibili dall'applicazione delle componenti sviluppate da due gruppi di lavoro tecnologici: work package 3 (dedicato al trattamento del segnale vocale ai fini di una sua migliore robustezza) e work package 4 (dedicato al contrasto delle tecniche utilizzate dagli impostori per "ingannare" i sistemi di riconoscimento vocale). Le prove sul campo saranno eseguite presso l'Aeroporto di Linate e Findomestic, secondo le linee-guida tecniche fornite dalla Fondazione, anche con riferimento a problematiche di usabilità e user experience, e in coerenza con i requisiti di business autonomamente fissati dalle due società. La Fondazione contribuirà a elaborare i risultati delle prove, al fine di desumere indicatori di prestazioni utilizzabili come elementi di valutazione delle prospettive di sfruttamento operativo e commerciale dei risultati. La Fondazione è anche impegnata (nell'ambito di uno specifico task del work package 3) sulla messa a punto di algoritmi per migliorare la environmental robustness del segnale vocale in ambienti rumorosi.

Nel 2016, la Fondazione ha avuto un ruolo di rilievo (coordinamento oppure contribuzione tecnica principale) nella produzione di cinque relazioni tecniche di progetto. La Fondazione ha contribuito anche a un Deliverable su metodi atti a massimizzare l'accuratezza dell'elaborazione del segnale vocale in ambienti rumorosi, fornendo algoritmi e realizzando i relativi moduli software in MathLab, per il filtraggio di alcune tipologie di rumore comuni nei campi di applicazione dei trial di progetto (rumore di aerei in fase di rullaggio, decollo e atterraggio, rumore di mezzi pesanti, rumore in un ambiente di ufficio). È stata anche condotta una campagna di valutazione soggettiva della qualità del segnale filtrato.

Comunicazione e diffusione dei risultati. Il sito ufficiale del Progetto (www.octave-project.eu) è stato aggiornato costantemente e in coerenza con lo stato di avanzamento dei lavori. È stato anche regolarmente presidiato l'account Twitter (@OCTAVE_H2020) associato al Progetto. Nel giugno 2016, OCTAVE ha avuto la sua prima presentazione pubblica, con uno stand istituzionale e dimostrativo nell'ambito della conferenza *Odyssey 2016* e con varie comunicazioni alla stessa conferenza. Nel settembre 2016, FUB è stata invitata a organizzare e presiedere una sessione di presentazione dei risultati di OCTAVE, con cinque relatori inviati dai Partner di Progetto, in occasione della Conferenza annuale della European Biometric Association, svoltasi a Darmstadt (Germania).

Output dell'attività di coordinamento e comunicazione

- OCTAVE Project: "Notifications to - and approvals from - National Data Protection Authorities" (final version), Deliverable D19, a cura della Fondazione Ugo Bordoni, gennaio 2016.
- OCTAVE Project: "Dissemination and communication plan", Deliverable D20, a cura del partner ATOS, con contributi della Fondazione Ugo Bordoni, maggio 2016.
- OCTAVE Project: "Report on communication actions and participationin events (Year 1)", Deliverable D21, a cura del partner ATOS, con contributi della Fondazione Ugo Bordoni, maggio 2016.
- OCTAVE Project: "Review Report for Year 1", documento preparatorio della prima verifica di Progetto da parte della Commissione, a cura della Fondazione Ugo Bordoni, che ha curato tutta la parte gestionale e tecnica di carattere generale e coordinato i contributi dei singoli WP e dei singoli Partner.

Output scientifici

- Falcone M., "Voice Biometrics from Research and Innovation to Reality", *EAB – Research Project Conference*, 20-21 settembre 2016, Darmstadt.
- Trigila S., "OCTAVE: Motives and Drivers for a Project Blending Secure Access Distributed Platforms and User Authentication by Voice Biometry", *EAB – Research Project Conference*, 20-21 settembre 2016, Darmstadt.
- Kinnunen T., Sahidullah M., Falcone M., Costantini L. et al. "RedDots Replayed: A New Replay Spoofing Attack Corpus for Text-dependent Speaker Verification Research", Proceedings of the *42nd IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, March 5-9, 2017, New Orleans, USA.
- OCTAVE Project: "Corpora Definition", Deliverable D13, a cura e con il contributo determinante della Fondazione Ugo Bordoni, gennaio 2016.
- OCTAVE Project: "Corpora Collection", Deliverable D17, a cura del partner ValidSoft e con il contributo determinante della Fondazione Ugo Bordoni, marzo 2016.
- OCTAVE Project: "Methods for environmental robustness", Deliverable D22, a cura del partner Aalborg University, con contributi della Fondazione Ugo Bordoni, maggio 2016.
- OCTAVE Project: "Spoofing Corpora", Deliverable D25, a cura del partner University of Eastern Finland, con il contributo determinante della Fondazione Ugo Bordoni, maggio 2016.
- OCTAVE Project: "Technology Baseline", Deliverable D15, a cura del partner ATOS, con contributi della Fondazione Ugo Bordoni, giugno 2016.
- OCTAVE Project: "Online Users Access Control Validation Report", Deliverable D34, a cura del partner Advalia, con contributi della Fondazione Ugo Bordoni, dicembre 2016.

ICT PER L'ENERGIA

RSE CYBERSECURITY

Ricerca sul Sistema Energetico - Cybersecurity

Progetto in convenzione con RSE

Il Progetto prevede attività di ricerca e studio per ciò che concerne gli aspetti relativi alla sicurezza ICT nel settore energetico, con particolare riferimento alle tecnologie di Demand Response (DR) utilizzabili nelle Smart Grid.

Obiettivi

Analizzare il contributo e l'impatto della sicurezza ICT in casi d'uso di tecnologie di Demand Response (DR) del contesto Smart Grid.

Impatto

Lo studio e l'applicazione dei protocolli definiti in ambito DR in specifici casi d'uso consente di verificare il soddisfacimento dei requisiti di sicurezza definibili per tali casi nonché di valutare l'impatto della sicurezza sulle prestazioni con le quali è possibile offrire i relativi servizi.

Descrizione

Il Progetto si inquadra nel contesto della collaborazione avviata con RSE nel 2015, finalizzata a svolgere attività di ricerca nel settore energetico per ciò che concerne gli aspetti relativi alla sicurezza ICT. Tali aspetti vengono in particolare analizzati nell'ambito delle tecnologie di Demand Response (DR) utilizzabili nelle smart grid per evitare squilibri nel bilanciamento tra domanda e offerta di energia. Ciò al fine sia di evitare pericolose situazioni di black-out sia di acquisire energia a prezzi più bassi e di consentire così l'applicazione di tariffe più convenienti all'utente finale. Utilizzando opportuni dispositivi (Aggregatore, EMG/CEM) in grado di comunicare tra loro, possono essere inviati all'utenza incentivi economici, non solo per distribuire i consumi su fasce orarie non critiche, ma anche per indurre l'utenza, qualora ne abbia la capacità, a immettere energia sulla rete nelle fasce orarie critiche (energia prodotta, ad esempio, da impianti fotovoltaici domestici). Il dispositivo installato presso l'utente e opportunamente programmato da quest'ultimo provvede poi ad accettare o meno l'offerta e a regolare di conseguenza, in caso di accettazione, i consumi o la produzione di energia. Le comunicazioni tra i dispositivi utilizzati nel DR sono in parte veicolate su rete pubblica e prevedono lo scambio di informazioni che devono essere protette dal punto di vista sia dell'integrità sia della riservatezza, ad esempio per tutelare la privacy dell'utente relativamente ai propri consumi di energia elettrica. Conseguentemente devono essere utilizzati protocolli di comunicazione in grado di offrire tale protezione. Il Progetto mira ad analizzare tali protocolli dal punto di vista della sicurezza ICT, a definirne le modalità di utilizzo in specifici contesti applicativi, ad individuare potenziali criticità e a fornire indicazioni circa eventuali verifiche del livello di sicurezza di dispositivi/sistemi reali. Rientra tra gli obiettivi del Progetto anche l'analisi dell'impatto delle tecniche di protezione previste nei protocolli DR sui ritardi temporali con i quali vengono scambiati i dati.

Attività 2016

Nel corso del 2016 sono state raffinate le analisi precedentemente eseguite sui temi della Cybersecurity e delle infrastrutture a chiave pubblica (PKI) nelle applicazioni di Demand Response. Per ciò che concerne il primo tema, l'analisi dei rischi precedentemente condotta per uno specifico caso d'uso (la ricarica di un veicolo elettrico) è stata inoltre estesa e raffinata rendendo più dettagliato il modello architetturale e integrando i risultati ottenuti in precedenza. È stata eseguita, inoltre, un'analisi dei rischi ipotizzando uno scenario di cyberterrorismo, nel quale vengono ipotizzati anche attacchi che non si limitino a rendere indisponibili le funzionalità DR, bensì mirino a servirsi di tali funzionalità per produrre risultati addirittura opposti rispetto a quelli per i quali sono state progettate. In altri termini attacchi che portino ad aggravare, invece che ad attenuare, le situazioni di squilibrio tra domanda e offerta di energia sulla rete elettrica, con l'obiettivo di provocare black-out più o meno estesi. Altra tematica trattata nelle attività del 2016 è quella delle verifiche del livello di sicurezza effettivamente realizzato in prodotti e servizi nel contesto smart-grid. Il livello di sicurezza effettivo che ci si può attendere in un contesto predefinito dipende sia dall'adeguatezza dei requisiti di sicurezza sia dalla severità delle azioni di verifica e dalla competenza e imparzialità dei soggetti incaricati di eseguirle. Nelle attività del 2016, sono state analizzate sotto i vari aspetti possibili le verifiche di sicurezza fino ad oggi definite nel settore della sicurezza ICT, al fine di facilitare il loro utilizzo nel contesto delle smart grid. Sono state inoltre descritte le verifiche del livello di sicurezza definite in uno degli ambiti del settore energetico, quello dei sistemi di controllo, per ciò che concerne sia i componenti di tali sistemi, sia i sistemi di gestione della sicurezza (ISMS). Infine, sono stati illustrati i risultati di attività svolte in Germania e in Turchia ai fini di una certificazione di sicurezza di sistemi di smart metering.

DELIVERABLE

- "Cybersecurity nel contesto Demand Response: approfondimenti e nuovi scenari di attacco".
- "Verifica del livello di sicurezza ICT nelle smart grid".

ICT PER L'ENERGIA

RSE QoS

Quality of Service per Servizi Smart Energy

Progetto in convenzione con RSE

Valutazione delle possibili soluzioni ICT in grado di promuovere lo sviluppo delle Smart Grid, basandosi su un'analisi tecnica/economica delle tecnologie disponibili o future e di come possano rispondere ai requisiti di QoS per il settore energetico.

Obiettivi

Individuazione degli scenari di reti TLC per il settore energetico. Scopo del Progetto è valutare l'adozione delle reti esistenti (2G-4G) e di quelle future, al fine di garantire il soddisfacimento dei requisiti di QoS necessari nei servizi previsti nelle Smart Grid.

Impatto

Il principale impatto del Progetto riguarda lo sviluppo delle Smart Grid nel contesto Europeo secondo le raccomandazioni promosse dal *Strategic Energy Technology Plan (SET-Plan)*. L'adozione dei sistemi ICT in ambito energetico contribuisce a promuovere e accelerare lo sviluppo delle tecnologie *low-carbon* per perseguire gli obiettivi fissati al 2030.

Descrizione

Il Progetto si occupa dello studio e dell'approfondimento scientifico degli aspetti ICT che abilitano servizi innovativi nel settore energetico.

Le attività svolte si possono dividere in 5 tematiche di approfondimento di seguito elencate:

1. Adozione delle 5G per servizi smart energy.
2. Valutazione delle Comunicazioni Machine-to-Machine (M2M Communications) per servizi Smart Grid.
3. Predisposizione di misure e test in collaborazione con il MiSE sulle reti di comunicazione per valutazioni di prestazioni per applicazioni nel dominio energetico.
4. Mappatura dei servizi di telecomunicazione a banda larga disponibili sul territorio nazionale.
5. Definizione di criteri metodologici e benchmark di servizi ICT per Smart Grid.

Attività 2016

Il Progetto è articolato secondo un piano triennale di attività. Nel 2016 sono stati affrontati i seguenti aspetti:

- Adozione delle 5G per servizi smart energy: individuazione dei principali KPI (Key Performance Indicator) da adottare nel settore "verticale" energia, al fine di stabilire i requisiti da soddisfare nell'erogazione degli Smart Energy Services.

- M2M: valutazione di connettività delle tecnologie abilitanti le comunicazioni M2M; analisi delle soluzioni embedded-SIM per applicazioni energetiche.
  - Valutazione connettività: tecnologie abilitanti comunicazioni M2M tramite simulazioni di propagazione radio in aree geografiche di riferimento con acquisizione dati siti reali operatori mobili. Per tali valutazioni si sono considerate sia soluzioni basate su banda licenziata (M2M Cellular Networks), quali e-MTC (enachend-Machine Type Communication), NB-IoT (Narrowband IoT), EC-GSM (Extended Coverage GSM); sia soluzioni Unlicensed LPWA (Low Power Wide Area) basate su scelte proprietarie, quali, SIGFOX e LoRa.
  - Valutazione delle Embedded-SIM per applicazioni Smart Energy considerando sia gli aspetti tecnici quali (analisi standard, Number Portability, funzionalità OTA), sia gli aspetti normativi (*Permanent Roaming* a livello nazionale e indagini a livello europeo).
- Predisposizione di misure e test in collaborazione con il MiSE (Ministero dello sviluppo economico) nell'ambito di sperimentazioni sulle reti di comunicazione per applicazioni nel dominio energetico.
- Sviluppo di un sistema informativo geografico per mappatura dei servizi di telecomunicazione a banda larga disponibili sul territorio nazionale.
- Valutazione delle reali disponibilità di copertura TLC disponibile sul territorio nazionale con i relativi livelli di qualità, per dotare la rete di Distribuzione Elettrica di servizi smart.
- Definizione di criteri metodologici e benchmark per la valorizzazione dei costi associati ai servizi di telecomunicazione nei progetti smart grid.

DELIVERABLE

- D1.1.2 "Definizione campagne di misura di reti TLC emergenti per implementare servizi Smart Energy Grid".
- D2.1.2 "Analisi di propagazione tecnologie radio per scenari di applicazioni Smart Grid".
- D2.2.2 "Valutazione e-SIM per servizi Smart Energy Grid".
- D3.1.2 "Definizione campagne di misura di reti TLC per implementare servizi SG".
- D4.1.2 "Analisi Costi/Benefici delle soluzioni SG nel contesto italiano".
- D5.1.2 "Descrizione interfaccia reti TLC-Atlante Integrato per mappatura reti di Telecomunicazioni ed Elettriche sul territorio nazionale".

SOFTWARE/TOOL

- S2.1.2: Mappe di copertura tecnologie per M2M.
- S5.1.2: Mappe di Copertura reti di TLC.

ICT PER L'ENERGIA

Mappatura M2M IOT - SMART CITIES

Progetto in convenzione con AGCOM (Delibera n. 626/16/CONS, ex Delibera n. 211/16/CONS abrogata)

Realizzazione di un sistema di elaborazione per il calcolo delle coperture Wireless delle tecnologie abilitanti M2M/IoT al fine di predisporre degli strumenti di supporto all'analisi comparativa delle diverse soluzioni per i servizi IoT.

Obiettivi

Elaborazione di mappe di copertura delle principali tecnologie wireless di accesso in vari ambienti (urbano, suburbano, rurale) per il riscontro delle prestazioni effettivamente raggiungibili dalle diverse soluzioni abilitanti applicazioni M2M/IoT.

Impatto

Lo studio proposto avrà un notevole impatto sulle scelte tecnologiche future in quanto effettua comparazioni delle diverse soluzioni abilitanti l'M2M al fine di dare indicazioni sulla potenziale capacità di ogni soluzione di garantire la connettività necessaria per implementare gli innovativi servizi IoT in ottica "smart city".

Descrizione

Lo studio riportato affronta l'analisi comparativa delle tecnologie abilitanti le comunicazioni M2M ad oggi disponibili. Esso prende in considerazione essenzialmente due diverse tipologie di tecnologie wireless di accesso:

- M2M Cellular Networks: soluzioni licenziate basate su reti mobili secondo lo standard 3GPP, partendo dalla soluzione consolidata 2G, alla sua evoluzione 3G, fino alle ultime Release della rete 4G.
- LWPA (Low Power Wide Area) Networks: soluzioni proprietarie espressamente sviluppate per applicazioni M2M/IoT (169 MHz, LoRa, SigFox) e quindi in grado di soddisfare i requisiti di estensione di copertura e di basso consumo di potenza.

Lo studio sperimentale è stato condotto presso la Fondazione Ugo Bordoni mediante un sistema di elaborazione proprietario in cui sono state introdotte tutte le caratteristiche geografiche del territorio e la propagazione del segnale è stata analizzata considerando i principali geotipi di riferimento (urbano, suburbano e rurale) e considerando diversi ambienti di propagazione (outdoor, indoor e "deep" indoor). Le simulazioni sono state elaborate considerando i siti reali dei principali operatori mobili operanti nel territorio nazionale.

Tale analisi consente di valutare la potenziale capacità di ogni soluzione proposta di garantire il collegamento con un dispositivo utente collocato in situazioni operative più o meno critiche, al fine di fornire le indicazioni di connettività necessarie per implementare i servizi IoT di futura generazione in ottica "smart city".

Attività 2016

Partendo da valutazioni tecniche sulle caratteristiche delle principali reti di accesso wireless e sui conseguenti aspetti regolamentari, sono state analizzate le prestazioni in termini di copertura radio delle possibili tecnologie in un contesto reale.

L'area di riferimento per l'analisi è stata la provincia di Bologna dove sono stati presi in considerazione i siti dei principali operatori mobili presenti nel territorio. Le valutazioni di propagazione sono state effettuate considerando scenari urbani, suburbani e rurali della Provincia di Bologna effettuando valutazioni in contesti outdoor, indoor e "deep indoor" (sottoscala e seminterrati) per simulare installazioni reali di dispositivi M2M.

La comparazione delle varie soluzioni è stata effettuata considerando come riferimento le soglie minime di ricezione di terminali di utente sia nel caso di dispositivi "tradizionali" sia per il caso di terminali specificatamente dedicati al M2M. Infine, per effettuare comparazioni di scenari reali, le valutazioni sono state predisposte sia considerando la copertura ottenuta da un singolo operatore attivo sul territorio, sia nel caso di roaming.

Dalle valutazioni si evince che nel caso di soluzioni proprietarie e per tecnologie licenziate e mature quali il 2G, il roaming non apporta un miglioramento significativo, mentre per soluzioni quali 3G e soprattutto 4G, che non hanno lo stesso grado di diffusione del 2G sul territorio, si apprezzano dei miglioramenti più consistenti.

DELIVERABLE

- Analisi tecnologie per applicazioni M2M/IoT.

SOFTWARE/TOOL

- Predisposizione dei dati GIS di copertura e implementazione di una web application per visualizzazione coperture wireless.

LABORATORI

- Predisposizione di un laboratorio virtuale AGCOM-FUB in cui il personale FUB ha accesso (con autenticazione) allo spazio condiviso sui server AGCOM per caricare ed elaborare dati congiuntamente con il personale AGCOM.

POLITICHE DELL'ICT

AGID: Piano triennale per l'informatica nella PA

Progetto in convenzione quadro con l'Agenzia per l'Italia Digitale

Il Piano triennale per l'informatica è il documento di programmazione strategica ed economica di tutta la PA italiana, che definirà un indirizzo unitario e una visione sistemica per lo sviluppo dei sistemi informativi.

Obiettivi

Redazione del Piano triennale per l'informatica nella PA, con l'obiettivo di un risparmio per il settore informatico del 50% della spesa corrente (nel triennio 2016-2018).

Impatto

Saranno individuati i principi architetturali fondamentali, classificate e razionalizzate le spese per amministrazione o categorie di amministrazioni. I risparmi ottenuti sul fronte della spesa corrente alimenteranno nuovi investimenti in innovazione e sviluppo.

Descrizione

La legge 28 dicembre 2015, n. 208 (Legge di stabilità 2016), all'art.1, comma 513 prevede che l'Agenzia per l'Italia digitale (AgID) predisponga il Piano triennale per l'informatica nella pubblica amministrazione, approvato dal Presidente del Consiglio dei ministri o dal Ministro delegato. L'obiettivo è quello di un risparmio di spesa annuale, da raggiungere alla fine del triennio 2016-2018, pari al 50% della spesa annuale media relativa al triennio 2013-2015, per la gestione corrente del solo settore informatico al netto dei canoni per servizi di connettività e della spesa effettuata tramite Consip SpA o i soggetti aggregatori. I risparmi derivanti dall'attuazione di tale disposizione saranno utilizzati dalle medesime Amministrazioni prioritariamente per investimenti in materia di innovazione tecnologica.

La FUB è stata coinvolta a vari livelli nelle attività di redazione dei documenti e delle linee guida per le PA.

Attività 2016

Nel corso del 2016, i contributi specifici della Fondazione hanno riguardato:

- analisi dei documenti elaborati dalla segreteria tecnica e dai gruppi di lavoro;
- decalogo per la pianificazione delle spese e investimenti in ICT;
- analisi impatto Open Data sugli investimenti, risparmi e incremento dell'occupazione;
- prima analisi e proposta di indicatori di performance per misurare ciò che viene realizzato con le risorse disponibili;
- contributo per gli aspetti relativi alla conservazione per nell'ambito del layer "infrastrutture materiali";

- attività di revisione e raccordo tecnico sui contributi forniti dagli uffici interni di AgID relativi ai vari temi trattati nel Piano triennale;
- coordinamento con i referenti interni AgID di cui al punto precedente;
- coordinamento con i referenti tecnici del Team per la Trasformazione Digitale, struttura istituita presso la Presidenza del Consiglio dal Commissario Straordinario per l'attuazione dell'Agenda Digitale.

POLITICHE DELL'ICT

AGID: ANPR

Anagrafe Nazionale della Popolazione Residente

Progetto in convenzione quadro con l'Agenzia per l'Italia Digitale

L'ANPR ha lo scopo di realizzare un'unica banca dati con le informazioni anagrafiche della popolazione residente a cui faranno riferimento i Comuni, la Pubblica amministrazione, i gestori di pubblici servizi, i soggetti e gli enti interessati a tali dati.

Obiettivi

Obiettivi del Progetto sono: la sostituzione delle oltre 8.000 anagrafi dei Comuni italiani, l'allineamento dei dati toponomastici, la realizzazione dell'Anagrafe nazionale dei numeri civici e delle strade urbane (ANNCSU), il completamento della riforma del Catasto, il supporto a CIE (Carta d'Identità Elettronica) e FSE (Fascicolo Sanitario Elettronico).

Impatto

La realizzazione dell'ANPR avrà un forte impatto sull'efficienza dei servizi resi dalle PA verso i cittadini, le imprese e all'interno delle stesse PA. Sarà possibile realizzare alcuni servizi che permetteranno di accelerare iter burocratici con un complessivo risparmio in termini di costi e di tempi di processamento. La centralizzazione dei dati e di tutte le applicazioni digitali collegate imprimeranno anche un forte impulso alla dematerializzazione e alla digitalizzazione della PA nel suo complesso.

Descrizione

L'ANPR è un Progetto svolto nell'ambito della convenzione tra AgID e FUB. Con l'ANPR verrà costituito un database unico nazionale delle anagrafi di tutti i Comuni italiani, includendo anche l'anagrafe degli italiani residenti all'estero (AIRE). Altri enti potranno stipulare delle convenzioni con il Ministero dell'interno per l'uso di tali dati, che saranno il riferimento unico per l'anagrafe italiana. L'ANPR sarà centrale per la realizzazione di progetti decisivi nel piano di lavoro dell'Agenda Digitale italiana.

Attività 2016

Sono state analizzate le diverse soluzioni digitali in precedenza adottate nei Comuni italiani per la gestione dell'anagrafe locale. FUB ha contribuito a sintetizzare le esperienze di tutti i Comuni per offrire una soluzione con continuità d'opera ma al contempo potenziabile in termini di cooperazione, nel senso di scambio dei dati anagrafici verso la PA e altri enti in generale, e di risparmio di risorse per i Comuni. Il tutto rafforzando le caratteristiche di sicurezza relative al trattamento di questo tipo di dati. Le attività svolte hanno portato alla definizione di punti d'intervento da parte di AgID per normalizzare le condizioni di subentro da parte dei vari Comuni pilota: ad esempio sono state individuate delle azioni condivise da tutti i Comuni, come la procedura di creazione dei messaggi SOAP secondo le specifiche ANPR, che possono essere coadiuvate dalla presentazione di codici sorgenti di riferimento. FUB ha inoltre partecipato, anche in veste di coordinatore e organizzatore, a tavoli tecnici con comuni, ministeri ed altri enti coinvolti nel processo. È stato anche formulato un questionario rivolto ai Comuni pilota, con l'obiettivo di evidenziare degli aspetti funzionali e tecnologici nei servizi anagrafici dei singoli Comuni utili alla pianificazione del subentro e a supporto delle scelte architetturali.

POLITICHE DELL'ICT

AGID: Conservazione

Progetto in convenzione quadro con l'Agenzia per l'Italia Digitale

Il sistema di conservazione garantisce autenticità, integrità, affidabilità, leggibilità e reperibilità dei documenti informatici, come previsto dal Codice dell'Amministrazione Digitale (CAD) (art.44).

Obiettivi

Istituzione per i documenti amministrativi pubblici, e relativi metadati, di un sistema di conservazione che assicuri la loro autenticità, integrità, affidabilità, leggibilità e reperibilità con l'adozione di regole, procedure e tecnologie.

Impatto

La conservazione ha lo scopo di proteggere nel tempo gli archivi di documenti informatici e i dati, assicurandone l'accesso anche oltre il loro ciclo di vita. Ciò comporterà la dematerializzazione progressiva della carta, con risparmi economici e di spazio e, al contempo, la reperibilità di vecchi documenti, di cui sarà impedita la perdita o la distruzione e saranno garantite l'autenticità e l'integrità, con accesso controllato ai fini amministrativi e di ricerca.

Descrizione

Per alcuni tipi di documenti amministrativi pubblici e relativi metadati, dev'essere definito un sistema di conservazione che assicuri, dalla presa in carico da parte del produttore fino all'eventuale scarto, la conservazione tramite l'adozione di regole, procedure e tecnologie che ne garantiscano le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità. L'AgID è incaricata di definire le modalità operative per realizzare tale attività di conservazione. La FUB collabora alla definizione delle funzioni del sistema e dei modelli organizzativi, partecipando a tutte le fasi dello svolgimento del Progetto.

Attività 2016

Nel 2016 sono state svolte le seguenti attività:

- definizione del glossario, dei formati, degli standard e delle specifiche tecniche del pacchetto di archiviazione, dei metadati;
- linee guida per la conservazione di mail con virus e log messaggi di posta elettronica;
- istruzioni per indirizzare le PA verso le possibili soluzioni di conservazione (in house, richiesta di servizi tramite gara Consip, ricorso ai conservatori accreditati e utilizzazione dei servizi dei poli di conservazione);
- analisi per la predisposizione di indicazioni dettagliate per gli ispettori incaricati della vigilanza e per i soggetti certificati incaricati di predisporre la certificazione di conformità;
- vigilanza e rilascio certificati di conformità;