PADIGITALE
INNOVAZIONE PER LA PUBBLICA AMMINISTRAZIONE
WEB TECHNOLOGY FOR A REAL INNOVATION

CONSERVATORE DI DOCUMENTI INFORMATICI



## Norme di Sicurezza e Adeguamento

Pieve Fissiraga, 14-02-2022

# Urbi Smart / WebTec / CDAN
# Qualificazione dei servizi SAAS e ottemperanza al GDPR (General Data Protection Regulation Regolamento UE 2016/679), così come disposto dal Decreto Legislativo 10 agosto 2018, n. 101

## Indice

## 1. Urbi Smart: Cloud Comuputing e licenza d'uso

**Urbi Smart è il sistema informativo gestionale e direzionale integrato, web nativo, con un'unica base dati, che ha rivoluzionato la gestione delle informazioni nella Pubblica Amministrazione**.

Urbi Smart è un unico strumento di supporto per il governo del Comune e degli Enti, accessibile da qualsiasi dispositivo mobile (essendo web nativo, si "muove" agevolmente in Internet) e in qualsiasi momento e luogo grazie alla modalità **CLOUD COMPUTING - di seguito Cloud -** definita anche SAAS (Software as a service) o ASP (Application Service Providing). Urbi Smart è per l'appunto disponibile nella modalità Cloud, ma può essere utilizzato anche nella tradizionale forma in licenza d'uso.

L'architettura web nativa - con accesso mediante qualsiasi PC con browser collegato a Internet o anche attraverso i più moderni strumenti mobile (come ipad Apple, tablet con Android oltre che iPhone, smartphone, palmari ecc.) - consente una naturale predisposizione verso il Cloud. Urbi Smart quindi si trova nella "nuvola informatica" (essendo in rete) e non risiede presso i server dell'ente che ne fruisce, ma in server dislocati presso un Internet Data Center (IDC) esterno sul territorio nazionale italiano. L'IDC di cui dispone PA Digitale S.p.A. (d'ora in avanti PA Digitale) risulta qualificato da AgID (Agenzia per l'Italia Digitale) come CSP - Tipo C così come imposto dalla normativa vigente.

Oltre ad essere in linea con le direttive dell'Agenzia per l'Italia Digitale (ex Digit PA, già CNIPA), tale modalità di erogazione consente di utilizzare soluzioni ad alto profilo tecnologico e costantemente aggiornate, protette e in grado di facilitare notevolmente l'interazione con i cittadini o altri soggetti esterni, senza forti investimenti infrastrutturali e pesanti costi di gestione (ad es. acquisto di software, hardware e infrastrutture di rete, costi di personale altamente specializzato per la gestione di infrastrutture complesse necessarie per usufruire della rete ecc.).

L'ente si avvale così anche **di un servizio specializzato che consente il ripristino rapido e completo dei dati in caso di interruzioni impreviste dei servizi e, quindi, la continuità operativa dei propri utenti** (in linea con quanto disposto dall'art. 50 del D. Lgs. 82/2005, Codice dell'Amministrazione Digitale - CAD).

**Attualmente oltre 850 Enti utilizzano Urbi Smart in modalità Cloud e oltre 100 in modalità on premise (licenza d'uso).**

La tecnologia web rende le applicazioni Urbi Smart estremamente efficaci, comunque, anche se acquisite in modalità licenza d'uso, in quanto sono tecnologicamente predisposte per essere installate in un proprio CED o presso altra server farm ed essere aperte alla rete internet. In questo contesto Urbi Smart si presta ad essere l'unica soluzione per aggregazioni di Comuni, CST, Comunità Montane che vogliono erogare i servizi direttamente dalla loro server farm o struttura CED.

## 2. WebTec: Cloud Comuputing

WebTec è la piattaforma **di servizi per la digitalizzazione di dati, attività e processi, sviluppata con tecnologia web**, che PA Digitale rivolge a Software House, Rivenditori, Produttori di software applicativi, Dealer, System Integrator per accompagnare i loro clienti - aziende, professionisti, associazioni di categoria, ordini professionali - verso la Digital Transformation, mantenendo una completa autonomia tecnica e di mercato nonché una gestione esclusiva del cliente.

Con WebTec, gli operatori ICT possono completare la loro offerta gestionale con nuovi **servizi perfettamente integrabili con i principali ERP e soluzioni gestionali, grazie a una ricca libreria di API rest**, per assicurare con la massima semplicità un colloquio applicativo e una gestione aziendale integrata con le soluzioni già in uso.

L'offerta dei servizi è veramente ampia, ideata per la massima semplicità e fruibilità grazie anche al pannello di gestione che consente l'attivazione di servizi e funzioni: **fattura elettronica** (*PA Digitale è soggetto accreditato SDI*), **gestore documentale e conservazione digitale a norma con workflow integrato e firma digitale, workflow processuale, servizi di integrazione con l'Agenzia delle Entrate, quadratura cassetto fiscale, gestione strutturata delle PEC, web mail, gestione pratiche, agenda mobile, prenotazioni on line degli appuntamenti, servizi di collaboration & communication per la condivisione di dati e documenti con clienti/associati, gestione corrispondenza, gestione del credito**.

Grazie al pannello di attivazione, accessibile anche in mobilità, è **sempre garantita quindi la possibilità di attivare nuove funzioni/componenti applicative e comporre così la proposta di servizi sulla base delle reali esigenze del clienti**.

WebTec è un **sistema unico** in cui le informazioni man mano si arricchiscono pur garantendo **l'unicità del dato** e dunque, senza duplicazione delle informazioni all'interno del DB dell'utente finale.

**Tutti i servizi sono fruibili in totale mobilità e in cloud**: il 100% delle funzioni è utilizzabile, per tutto il sistema e per qualsiasi utente, da un qualsiasi luogo e con qualsiasi device, ottenendo così una totale mobilità. I servizi WebTec sono quindi disponibili 24 ore su 24, 365 giorni all'anno e sono costantemente aggiornati prevedono aggiornamenti e backup "a caldo", senza alcun costo infrastrutturale e di gestione.
**Gli oltre 300.000 utenti finali e 70.000.000 di fatture elettroniche gestite ogni anno**, per esempio, testimoniano la solidità del sistema che rende i dealer veri protagonisti dell'innovazione digitale.

## 3. Servizio di Conservazione Digitale a Norma CDAN

Il Servizio di Conservazione Digitale a Norma **CDAN** di PA Digitale, preposto alla conservazione dei documenti informatici dei Clienti, è stato **realizzato con le tecnologie più innovative** e **in conformità alle regole tecniche di cui all'art. 71 del Codice dell'Amministrazione Digitale** (CAD), la cui rispondenza è requisito indispensabile ed essenziale per la corretta conservazione a norma dei documenti informatici.
**Il servizio CDAN assicura la conservazione digitale dei documenti informatici secondo le vigenti disposizioni di legge, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità e reperibilità** e mantenendo così inalterato nel tempo **il valore legale** dei documenti conservati.
Grazie ai numerosi automatismi e all'integrazione nativa con le applicazioni Urbi Smart e WebTec, la conservazione digitale a norma garantisce la **massima semplicità di gestione** per gli utenti, agevolati da **funzionalità immediate e da una grafica piacevole e intuitiva**. Tutti gli accessi al sistema, sia da parte degli utenti sia per le operazioni automatizzate di conservazione, avvengono in totale sicurezza tramite l'utilizzo di canali di comunicazione sicuri.
Il Servizio di Conservazione Digitale a Norma CDAN è erogato in modalità Cloud Computing come SaaS (Software as a Service) per i Clienti del Mercato Pubblico e Privato ed è conforme alle recenti *Linee guida sulla formazione, gestione e conservazione dei documenti informatici e relativi allegati* pubblicate da AgID. Il Servizio di Conservazione Digitale a Norma CDAN applica quanto previsto dal *Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici* e dai relativi Allegati A e B.

## 4. Le Certificazioni di PA Digitale

La modalità di applicazione di quanto descritto nel presente documento è governata da Procedure Operative Interne e da Istruzioni di Lavoro previste dal Sistema di Gestione Integrato per le norme ISO adottate da PA Digitale e certificato da un ente terzo indipendente, accreditato da Accredia, per l'ambito *Analisi, progettazione, sviluppo, produzione, installazione, commercializzazione, distribuzione, manutenzione e assistenza di prodotti software per la Pubblica Amministrazione Locale e Centrale e per il Mercato Privato, erogati in modalità SaaS oppure erogati con installazione in locale (on premise). Erogazione di servizi professionali connessi ai prodotti software per la Pubblica Amministrazione. Erogazione dei servizi SaaS in cloud per la Conservazione Digitale di documenti informatici a Norma e relativo servizio di assistenza.*
Le norme a cui PA Digitale attualmente aderisce sono

- UNI EN ISO 9001:2015 - Sistemi di Gestione per la Qualità - Requisiti, i cui dettagli sono illustrati nella Politica Aziendale della Qualità, pubblicata sul sito istituzionale di PA Digitale e raggiungibile nella sua versione più aggiornata al link https://www.padigitale.it/certificazioni/
- UNI CEI EN ISO/IEC 27001:2017 - Tecnologie Informatiche - Tecniche per la Sicurezza - Sistemi di gestione per la sicurezza delle informazioni - esteso alle Linee Guida: ISO/IEC 27017:2015 e ISO/IEC 27018:2019, i cui dettagli sono illustrati nella Politica Aziendale della Sicurezza delle Informazioni, pubblicata sul sito istituzionale di PA Digitale e raggiungibile nella sua versione più aggiornata al link https://www.padigitale.it/certificazioni/

I Sistemi di Gestione sono integrati con la Politica Aziendale in Materia di Trattamento e Protezione dei Dati Personali pubblicata sul proprio sito istituzionale al link https://www.padigitale.it/privacy/.

I servizi SaaS Urbi Smart e CDAN sono conformi alle Circolari AgID n. 2 e 3 del 9 aprile 2018 e pertanto sono presenti nel *Catalogo dei servizi Cloud qualificati per la PA* ai link:

- https://catalogocloud.agid.gov.it/service/494 (Urbi Smart),
- https://catalogocloud.agid.gov.it/service/1530 (CDAN).

PA Digitale eroga il Servizio di Conservazione Digitale certificato in conformità:

- alla Norma UNI EN ISO 9001:2015 - Sistemi di Gestione per la Qualità - Requisiti.

- alla Norma UNI CEI EN ISO/IEC 27001:2017 "Tecnologie informatiche - Tecniche per la sicurezza - Sistemi di gestione per la sicurezza delle informazioni - Requisiti". Il Sistema di Gestione della sicurezza delle informazioni soddisfa i criteri contenuti nelle seguenti Linee Guida: ISO/IEC 27017:2015 e ISO/IEC 27018:2019.
- ai requisiti individuati il servizio di "Conservatore di documenti informatici ai sensi dell'art. 29, comma 1, del D.Lgs. 7 marzo 2005, n. 82" e ss.mm.ii, tra cui si citano (a titolo esemplificativo e non esaustivo) le "Linee Guida sulla formazione, gestione e conservazione dei documenti informatici" (Agid Determinazioni 407/2020 e 371/2021, con applicazione dal 1° gennaio 2022) e il "Regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici" (Agid Determinazione 445/2021, in vigore dal 1° gennaio 2022).

Per tali ragioni, dal 14/02/2022 il Servizio di Conservazione Digitale a Norma **CDAN risulta qualificato presso AgID** mediante l'avvenuta iscrizione al Marketplace dei servizi di conservazione della società PA Digitale S.p.A. ai sensi dell'articolo 34 comma 1-bis lettera b) del decreto legislativo 7 marzo 2005, n. 82 e s.m.i., recante il Codice dell'amministrazione digitale (CAD). La qualificazione è consultabile al link: https://conservatoriqualificati.agid.gov.it/?page_id=276.

PA Digitale adotta un Codice Etico e un Modello di Organizzazione, Gestione e Controllo ai sensi del D. Lgs. 231/01, disponibili in consultazione sul sito istituzionale www.padigitale.it.

Si aggiunge infine che PA Digitale ha ottenuto un punteggio di **++ (tra i più alti degli operatori di settore) nel rating di legalità pubblicato dall'Autorità Garante della Concorrenza e del Mercato "AGCM". L'Elenco delle imprese con rating di legalità aggiornato e consultabile è reso disponibile dall'AGCM sul proprio sito al link https://www.agcm.it/competenze/rating-di-legalita/rating-elenco-imprese.

## 5. Cloud: vantaggi

Oltre alla possibilità di accedere ovunque alle applicazioni, l'utilizzo delle soluzioni erogate da PA Digitale in modalità Cloud (Urbi Smart, WebTec e CDAN) consente di avere molti vantaggi:

- Nessuna necessità di competenza informatica per la gestione di hardware, software e degli archivi.
- Nessun limite connesso alla necessità di dimensionamento del sistema: non occorre infatti stabilire a priori il dimensionamento dell'hardware, dato che, anche al crescere delle esigenze occorre esclusivamente aggiungere i posti di lavoro utente necessari.
- Nessun vincolo hardware e software.
- Totale eliminazione della responsabilità di archiviazione dei dati.
- Nessun vincolo contrattuale per l'eventuale cambio di fornitore.
- Estrema scalabilità.
- Aggiornamenti del software applicativo immediatamente disponibili.

## 6. Ottemperanza al Regolamento UE 2016 / 679 (GDPR) e relative misure di sicurezza (art. 32)

PA Digitale si impegna a rispettare sempre quanto previsto dal Regolamento UE 2016 / 679 (GDPR), e con particolare perizia quando è nominata Responsabile esterno del trattamento dati (oppure Sub responsabile esterno del trattamento dei dati). Nello specifico, adotta tutte le seguenti misure per ottemperare a quanto previsto dall'art. 32; dette misure (messe in esercizio da PA Digitale per garantire tanto l'Ottemperanza al GDPR quanto i più alti standard di sicurezza per le proprie soluzioni) sono illustrate nei capitoli seguenti.
Per i clienti che usufruiscono delle soluzioni Urbi Smart e WebTec - erogate in modalità Cloud - sono valide le misure descritte in ciascuno dei capitoli seguenti.
Per i clienti che usufruiscono della soluzione Urbi Smart erogata in modalità on premise (licenza d'uso) sono valide le misure descritte in ciascuno dei capitoli seguenti (fatta eccezione per l'intero capitolo 7 e per il paragrafo 9.2).
Infine, i clienti che usufruiscono della soluzione CDAN riterranno valide tutte le misure seguenti, eccetto che per alcuni paragrafi del capitolo 8 (8.1.b, 8.1.c, 8.1.d, 8.1.e - essendo CDAN una soluzione integrata con Urbi Smart e WebTec, ne eredita per queste parti le relative misure di sicurezza), per il paragrafo 9.2.

## 7. Sicurezza dei dati e continuità operativa

PA Digitale eroga i servizi Cloud - riportati ai capitoli 1, 2 e 3 - attraverso un Internet Data Center certificato in base al vigente standard internazionale ISO/IEC 27001 e alle Linee Guida ISO/IEC 27017 e ISO/IEC 27018, in cui le apparecchiature per la trasmissione dei dati e le architetture hardware/software preposte all'erogazione dei servizi sono poste in condizioni di massima **sicurezza applicativa e fisica** (sistemi antintrusione, sistemi antincendio, controllo accessi, telesorveglianza ai piani; ridondanza dei sistemi elettrici e di refrigerazione), **informatica e logica** (sistemi antintrusione).

Relativamente alla sicurezza fisica e infrastrutturale, l'Internet Data Center è dotato di protezione contro ogni minaccia, per garantire la massima sicurezza a dati e servizi. I sistemi di backup dei dati, il Disaster Recovery, la continuità dei servizi, offrono agli utenti i più elevati livelli di servizio, 24 ore su 24, 7 giorni su 7, 365 giorni all'anno. Tali garanzie sono fondamentali e indispensabili per gli Enti, sia per rispondere agli obblighi di legge in materia di **Business Continuity** (già citato art. 50, D. Lgs. 82/2005 - CAD), sia per poter garantire il corretto e regolare svolgimento della vita di cittadini e imprese nel caso di servizi in modalità online.

A tal fine, PA Digitale garantisce un servizio di **Disaster Recovery** completamente automatizzato in tutti i suoi processi e monitorato da personale tecnico specializzato 24 ore su 24, 7 giorni su 7, 365 giorni all'anno. Tutti i sistemi e apparati di rete/strutturali sono in configurazione fault-tolerance per evitare Single Point of Failure. La capacità di elaborazione del sistema di Disaster Recovery permette, in caso di disastro, il ripristino dell'erogazione dei servizi con prestazioni equivalenti al sito di normale operatività, in tempi conformi al Tier 3 e a quanto indicato al paragrafo sottostante *7.7 Servizi di backup e Disaster Recovery*. Attività di verifica e test di funzionamento dei sistemi sono svolte regolarmente per la massima sicurezza di dati e sistemi.

Il sito primario di erogazione servizi Cloud è presso il Data Center di Westpole S.p.A., in Via Francesco Sforza 13, Basiglio (MI). Il sito secondario di Disaster Recovery è presso il Data Center di Westpole S.p.A. in Via di Macchia Palocco 243, Acilia, Roma (RM).

Nel rispetto delle Circolari AgID n. 2 e 3 del 9 aprile 2018, l'IDC risulta qualificato come CSP - Tipo C ed è iscritto nel *Registro dei CSP Qualificati* consultabile al link https://catalogocloud.agid.gov.it/.

## 7.1 Internet Data Center

Le reti Metropolitane per i due Data Center (sito primario e sito secondario, citati al paragrafo precedente) si basano sulla cablatura in fibra la cui banda complessiva è di alcuni Gbps con possibilità di ampliamento immediato senza modifiche infrastrutturali. Il collegamento verso la rete pubblica internet viene garantito attraverso router di backbone con attestati i link di diversi operatori. Il protocollo di routing BGPV4, costantemente gestito sui router di backbone, decide le destinazioni selezionando il carrier con la miglior qualità di servizio da e verso specifiche aree geografiche. In caso di disservizio di uno dei carrier, il BGP provvede automaticamente a instradare tutto il traffico verso l'operatore funzionante e, se necessario, anche transitando per la connettività attestata sul sito secondario rispetto al Data Center che sta erogando il servizio.

I due Data Center sono connessi tra di loro da una dorsale in fibra, permettendone la gestione come fosse un "unico" Data Center distribuito. Il sistema di controllo degli accessi prevede una postazione di guardiania che identifica il personale che richiede accesso e fornisce badge che consente l'accesso alle sole aree di pertinenza.

## 7.2 Infrastruttura di sistema

L'**architettura del Data Center** è basata su componenti le cui principali caratteristiche sono:

- utilizzo di sole componenti di classe Enterprise;
- affidabilità delle singole componenti scelte;
- ridondanza fisica di tutti i componenti HW;
- ridondanza dei componenti SW di sistema e networking.

La disponibilità effettiva dell'infrastruttura presenta un uptime del 99.95%, garantita a diversi livelli sia grazie alle scelte architetturali che alle tecnologie utilizzate. Per garantire la massima disponibilità e fruibilità delle risorse atte all'erogazione dei servizi in modalità Cloud, PA Digitale monitora periodicamente le proprie risorse infrastrutturali predisponendo un Piano di Capacità/Capacity Plan con revisione minima annuale. Scopo di detto Piano è assicurare in ogni momento la capacità sufficiente per garantire il più alto livello di erogazione dei servizi in Cloud, in base alle attuali e future esigenze di business del mercato. Il Piano viene inoltre aggiornato in seguito a cambiamenti significativi del personale, dell'organizzazione o delle infrastrutture.

## 7.3 Sottosistema di virtualizzazione

I servizi sono erogati da un cluster di sistemi ad alta affidabilità VMware Enterprise in regime di Private Cloud, con risorse computazionali dedicate al fine di prevenire condivisione di risorse con altri ambienti. Alcune delle caratteristiche salienti:

- Vmotion: consente di migrare real time le VM tra host fisico a un altro cluster;
- Storage Vmotion: rilocazione di VM fra datastore senza interruzione del servizio;
- High Availability: in caso di failure di un host virtualizzatore o della VM.

## 7.4 Sottosistema storage

Per eliminare ogni rischio di interruzione del servizio dovuto a guasti HW, tutti i dischi delle VM e dei dati sono memorizzati esclusivamente su **SAN ad alte prestazioni dedicate al servizio**.
La configurazione della SAN garantisce assenza di Single Point of Failure, tutti i sistemi sono in costante monitoraggio che garantisce tempi di sostituzione componenti hardware senza completo fermo del sistema.
Le garanzie:

- **alta affidabilità dei componenti fisici**, tutti i componenti sono ridondati, cioè disco in RAID5 + hot-spare, SAN dual-fabric ecc.
- **scalabilità verticale e orizzontale dell'infrastruttura,** che è in grado di supportare richieste di workload e di spazio addizionale evitando situazioni di overbooking.

## 7.5 Sottosistemi firewall e componenti di sicurezza

L'architettura di sicurezza e firewall è implementata utilizzando **due firewall in cluster HA**, per la gestione dell'accesso internet e per la gestione della DMZ e LAN interna.
I server applicativi utilizzano **VLAN** per ottenere una separazione del livello database da quello applicativo, al fine di elevare la sicurezza di gestione dei documenti e di ridurre al minimo il rischio di compromissione dei sistemi in caso di attacco.
L'infrastruttura dispone di **sonde IPS** (Intrusion Prevention System) che garantiscono una protezione perimetrale da attacchi, per esempio di tipo DDOS (Distributed Denial of Service), di sonde antivirus per l'analisi di tutto il traffico web e per prevenire l'eventuale infezione causata da malware.
La sicurezza di accesso ai componenti del sistema è garantita attraverso l'uso di password a criptazione forte.
L'accesso all'IDC da parte di PA Digitale ai sistemi per scopi di amministrazione avviene attraverso connessioni **VPN** autenticate attraverso username/password e certificati digitali, oppure tramite VPN site 2 site IPSEC configurata direttamente fra i firewall di PAD e del sito primario. In quest'ultimo caso, è prevista un'ulteriore abilitazione specifica a livello di firewall.

## 7.6 Politiche di backup

Le politiche di backup adottate prevedono la gestione di tutti i dati relativi a Urbi Smart, WebTec e CDAN: database, documenti e componenti applicative. I backup hanno frequenza giornaliera e retention/storico di 30 giorni. I job di backup non impattano l'erogazione dei servizi; i backup dei database avvengono a caldo sul nodo del cluster "slave".

## 7.7 Servizi di backup e Disaster Recovery

La strategia di backup adottata per l'adozione delle Politiche descritte al punto precedente prevede l'implementazione e l'utilizzo di Veeam Backup and Replication e di NAS Platform Snapshots.
Le soluzioni adottate permettono il recupero dei dati, garantendone un corretto processo di ripristino e l'identificazione dei dati necessari recuperando il supporto di backup appropriato.
Sono pianificate delle prove di ripristino dei dati in maniera randomica, che consistono nel restore di un ambiente virtuale in un'area di test e le relative verifiche di buon funzionamento. La granularità dei backup relative ai database consente il recupero a livello del singolo record a una data specifica.
Il Disaster Recovery è gestito con tecnologia VMware Site Recovery Manager. Il sistema garantisce una procedura di disaster recovery con RPO di 4 ore ed RTO minimo di 4 ore e massimo di 48 ore.

## 8. La gestione della sicurezza e sistemi di security management per le procedure applicative

La gestione della sicurezza costituisce una tra le componenti più delicate nell'ambito, più generale, della gestione dei dati dei Clienti. Sia l'infrastruttura che i servizi SaaS erogati in modalità Cloud da PA Digitale sono periodicamente sottoposti ad attività di Vulnerability Assessment e Penetration Test, effettuati da un ente terzo indipendente certificato da Accredia.
Dovendo implementare un IDC per l'erogazione dei servizi di amministrazione degli enti in modalità Cloud, PA Digitale ha da tempo sviluppato e attuato una metodologia per l'analisi dei rischi legati alla sicurezza e alla sua gestione attraverso opportuni meccanismi e strumenti di controllo e di intervento.
Le scelte adottate, in linea con quanto enunciato dall'Agenzia per l'Italia Digitale in materia di sicurezza, portano a:

- controllo e monitoraggio degli accessi in modo puntuale e nel tempo;
- identificazione di eventuali anomalie;
- intervento nel minor tempo possibile per ripristinare la situazione correttamente.

## 8.1 Principi applicabili al legittimo trattamento dei dati

Per soddisfare i requisiti di sicurezza, le soluzioni Urbi Smart, WebTec e CDAN osservano principi applicabili al legittimo trattamento dei dati (con particolare riguardo verso le Informazioni Personali Identificabili - PII), supportando una serie di servizi e di dispositivi atti a implementare funzioni di autenticazione, autorizzazione e crittografia. Tali servizi e dispositivi risultano adeguati alla nuova normativa UE 2016/679 in vigore dal 25.05.2018, così come disposto in Italia dal Decreto Legislativo 10 agosto 2018, n. 101 "Disposizioni per l'adeguamento della normativa nazionale alle disposizioni del regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati)".
L'**autenticazione** prevede che gli utenti si debbano identificare con una serie nota di credenziali, ad esempio nome utente e password. Per i servizi on line di Urbi Smart è prevista a norma di legge l'autenticazione con le principali piattaforme ministeriali e regionali, che implementano SPID, CIE e CNS.
Per **autorizzazione**, invece, si intende l'assegnazione di determinati livelli di accesso al sistema, che si riflettono in ben identificate capacità operative sul sistema medesimo da parte del singolo utente correttamente identificato.
L'attribuzione dei privilegi degli utenti, intesi come regole sia di autenticazione che di autorizzazione, sono esclusivamente demandate all'Amministratore applicativo. Quest'ultimo può decidere se applicare su altri utenti i privilegi che regolano le policy di sicurezza, di accesso, visibilità e gestione dei dati.
La **sicurezza** dei dati è garantita:

- durante la fase di comunicazione client e server tramite utilizzo di protocollo https e crittografia di tipo TLS 1.2 o superiori
- nello storage all'interno del database
- durante la fase di comunicazione tra sottosistemi di infrastruttura (webserver, long run process server, dbms server, NAS) o applicativi (comunicazioni da/verso sistemi ministeriali e/o di terze parti mediante identificazione degli enti coinvolti nello scambio dei flussi informativi e degli utenti abilitati all'accesso ai servizi anche tramite l'utilizzo di certificati digitali).

I servizi sono sottoposti a controllo costante dell'erogazione e delle prestazioni del servizio mediante strumenti di supervisione, accessibili via web dal personale abilitato.
Di seguito le caratteristiche del gestionale espresse in forma sintetica che saranno dettagliate nei paragrafi successivi.

a. Erogazione servizio tramite protocollo https
b. Accessi al software protetti da "nome utente" e "password".
c. password di accesso "sicure".
d. Gradi di libertà predisposti in base alla profilazione ruoli degli utenti.
e. Protezione dei dati
f. Tracciabilità dei log di accesso per eventuali comunicazioni di Data Breach.
g. Tracciabilità delle variazioni ai dati del sistema

Infine, PA Digitale ha pubblicato la propria *Politica in Materia di Trattamento e Protezione dei Dati Personali* sul suo sito istituzionale, raggiungibile nella sua versione più aggiornata al link https://www.padigitale.it/privacy.

## 8.1.a Erogazione servizi mediante protocollo HTTPS

Sia i servizi di backoffice che i servizi on line di Urbi Smart, WebTec e CDAN possono essere erogati mediante protocollo HTTPS.
Il protocollo HTTPS consiste nel far transitare la comunicazione tramite il protocollo HTTP all'interno di una connessione criptata dal Transport Layer Security (TLS) 1.2 o superiori. Viene utilizzato per garantire trasferimenti riservati di dati nel web, in modo da impedire intercettazioni dei contenuti. Il principio che sta alla base di HTTPS è quello di avere:

- un'autenticazione del sito web visitato
- protezione della privacy
- integrità dei dati scambiati tra le parti comunicanti.

## 8.1.b Accessi al software protetti da nome utente e password

Urbi Smart, WebTec e CDAN utilizzano un sistema di **autenticazione basato su sessione**. Ogni programma all'interno delle tre soluzioni verifica la validità della sessione in corso (identificata da un token di sessione) prima di fornire la pagina richiesta. Allorché la sessione sia scaduta o non sia attiva, qualsiasi richiesta viene ridirezionata al sistema di autenticazione. Il sistema di autenticazione standard prevede autenticazione basata su **Login e Password.**
L'utente è identificato all'interno di una base dati da un *nome utente* e da una *password*, secondo lo schema seguente:

- login: nomeutente@identificativodb
- password: Password_Utente

Nomeutente, identificativodb e password sono gli elementi essenziali e univoci per procedere alla validazione di un utente.
Su richiesta, sono disponibili integrazioni a strumenti di autenticazione standard (es. LDAP, Active Directory) attraverso cui ricondursi a utenti censiti in Urbi Smart e WebTec.
Come già anticipato, per i servizi on line di Urbi Smart è prevista a norma di legge l'autenticazione con le principali piattaforme ministeriali e regionali, che implementano SPID, CIE e CNS.

## 8.1.c Password di accesso sicure

Le password sono tutte crittografate; ad ogni utente, l'Amministratore applicativo può assegnare:

1. **Data Scadenza Utente**: questa data indica la data fino alla quale l'utente è valido. **Scaduta questa data l'utente viene disattivato**. Questa data serve per consentire di attivare un utente per un certo periodo di tempo: se si lascia il campo vuoto, oppure impostato a valore infinito 31-12-9999, l'utente è sempre attivo.
2. **Password d'Ufficio**: se non diversamente specificato, l'utente è costretto a modificare la password la prima volta che entra nella procedura.
3. **Data Attivazione Password:** questa data (impostata di default al giorno di creazione dell'utente) indica la data di attivazione della password per l'utente. In alcuni casi può essere utile attivare gli utenti in date posteriori alla creazione dell'utente stesso.
4. **Giorni Validità Password:** indica per quanti giorni la password di un utente è valida, a partire dalla data di attivazione. Questo campo è utile per definire un periodo di validità della password all'interno del range definito tra la data attivazione e la data scadenza. L'Amministratore applicativo può decidere la policy utente alla scadenza dei giorni di validità. Le due scelte possibili sono: a) Costringere l'utente a cambiare password b) disattivare l'utente.
5. **Max Giorni Non Loggato:** indica il numero massimo di giorni in cui un utente può restare attivo senza accedere a Urbi Smart e WebTec. Trascorso tale numero di giorni senza che l'utente acceda al sistema, la procedura lo disattiva in automatico.

All'atto della creazione di un nuovo utente, l'Amministratore gli attribuisce:

1. la **Password** (di default viene impostata come password d'ufficio)
2. la **Data di Scadenza Utente**
3. la **Data di Attivazione della Password** (impostata alla data del giorno) e il numero di **Giorni di Validità della Password**
4. il numero **Max Giorni Non Loggato** (se si vuole che venga disattivato l'utente che non accede a Urbi Smart e WebTec per più di un certo numero di giorni consecutivi).

La prima volta che il nuovo utente entra nella procedura deve utilizzare la password attribuita dall'amministratore. Se la password assegnatagli è una **password d'ufficio**, il sistema gli presenta in automatico la sezione per il cambio password obbligatorio: **l'utente deve inserire una nuova password compresa tra 8 e 30 caratteri (almeno 2 numeri e almeno 5 lettere dell'alfabeto ed almeno un carattere tra . ; $ ! - < > )**. Modificata la password può

ritornare a Urbi Smart e WebTec tramite link contenuto nella maschera. Se l'utente sbaglia le credenziali per tre volte consecutive viene disabilitato, e può essere riabilitato solo mediante l'intervento dell'Amministratore, che agirà sempre attraverso l'interfaccia di gestione utenti. Il numero minimo di tentativi disponibili per tentare l'accesso è settato a 3, ma l'Amministratore applicativo può decidere di aumentare questo valore, secondo le politiche interne al cliente.

Un utente viene inoltre disabilitato se:
1. è scaduto (**Data Scadenza Utente** scaduta)
2. è stato per **MaxGiorniNonLoggato** senza accedere a Urbi Smart e WebTec (se tale valore è stato settato).
3. la sua password è scaduta (**Giorni Validità Password**, settato) ed è stato definito che alla scadenza l'utente debba essere disattivato.

Anche in questi casi è necessario riabilitarlo tramite l'intervento dell'Amministratore, come sopra.
L'**annullamento** di un utente prevede di annullare logicamente l'utente medesimo, in modo da garantire che le credenziali di autenticazione non saranno mai più utilizzate per diversi utenti, neppure in tempi diversi. Un utente **ANNULLATO** viene ancora visualizzato nella lista degli utenti (in apposita sezione), ma non è più attivo e non è più possibile effettuare operazioni su di esso. In questo modo si garantisce che non sarà mai inserito un utente con lo stesso nome di un utente già utilizzato in precedenza (anche se annullato).

## 8.1.d Gradi di libertà predisposti in base alla profilazione ruoli degli utenti.

Urbi Smart e WebTec permettono la definizione di tre tipologie di utenti in funzione della loro visibilità ed accessibilità alle varie procedure, e quindi in funzione del tipo di menù assegnato. In particolare:
1. **Utente Standard**: l'utente può entrare nell'area delle procedure abilitate e accedere di default a tutti i programmi raggiungibili in virtù del suo Profilo Primario (Visione, Gestione, Supervisore). È tuttavia possibile prevedere un ulteriore livello di autorizzazione, disabilitando l'accesso solo ad alcuni programmi.
2. **Utente Scrivania**: questo tipo di utente può accedere esclusivamente ai programmi che gli sono stati espressamente abilitati. L'utente Scrivania può accedere a Urbi Smart e WebTec solamente alle procedure che gli sono state assegnate, e la pagina di accesso proposta contiene soltanto i programmi che gli sono stati assegnati (non ha la navigazione completa dell'utente Standard).
3. **Utente Misto** (valido solo per Urbi Smart): è l'utente che è Standard per alcune procedure e Scrivania per altre. Ad esempio: un utente standard dell'anagrafe (che ha a disposizione tutte le scelte del menù anagrafico) al quale viene attivata la sola funzione di visualizzazione delle delibere o visualizzazione dei protocolli.

È possibile prevedere ulteriori autorizzazioni relative a specifiche applicazioni Urbi Smart e WebTec.
Tutti i programmi Urbi Smart e WebTec, al momento del rilascio, sono suddivisi per singole Procedure e ciascuno di essi viene rilasciato con un livello di accesso di default scelto fra tre tipologie di Programma: Programma di Visione, Programma di Gestione o Programma di Supervisore. Analogamente, eventuali Funzioni associate ai programmi stessi sono rilasciate con un valore di default fra Funzione Abilitata o Funzione Disabilitata.

Urbi Smart e WebTec prevedono la gestione delle abilitazioni organizzata a livelli:
- a livello di Procedura, relative a tutti i programmi della procedura;
- a livello di Programma, con accesso al programma, inserimento di dati, annullamento di dati, variazione di dati;
- abilitazioni all'interno del programma di particolari Funzioni.

Di conseguenza, sono previsti tre livelli di intervento per la definizione dei privilegi utente:
- associazione di uno dei Profili di Base previsti (a livello di procedura);
- abilitazione o meno dello specifico programma;
- abilitazione del programma con inibizione o meno di specifiche funzioni.

Nella tabella seguente sono evidenziate le abilitazioni di default sui programmi di una procedura in funzione dei Profili di Base di un utente:

| Profilo Base | Abilitazione di default dei programmi della procedura |
|---|---|
| Visione | Solo programmi definiti come Visione |

| | |
|---|---|
| Gestione | Programmi definiti come Visione e Gestione |
| Supervisore | Programmi definiti come Visione, Gestione e Supervisore |
| Scrivania | Solo programmi esplicitamente assegnati |

**Controllo interventi sui soggetti**
Il soggetto, sia esso una persona fisica o un soggetto giuridico, acquisisce in Urbi Smart e WebTec un'importanza elevata. Costituendo il punto centrale di indagini nell'ambito del sistema informativo ed essendo presente una sola volta come codice e relativo corredo anagrafico, necessita di una serie di controlli capillari sul trattamento delle sue informazioni. Due sono le sezioni previste per il controllo degli interventi sui soggetti: Variazione e Annullamento. Ogni variazione inerente a quello che è stato definito corredo anagrafico di un soggetto (fanno parte di questo gruppo per esempio cognome, nome, data nascita, codice fiscale) viene concessa esclusivamente se l'utente che vuole effettuare è autorizzato a compiere una Variazione e/o un Annullamento.
**Gestione classi di utenti**
La funzione è stata progettata per rendere più efficiente e ottimizzata la gestione delle profilazioni degli utenti. È possibile identificare una serie di utenti di riferimento (utenti di tipo classe) e permettere a tutti gli utenti collegati a una classe di ereditare le caratteristiche dell'utente capofila o di riferimento. Grazie a tale impostazione, è possibile effettuare estrazioni o applicare filtri esclusivamente a determinate classi di utenti.
**Gestione stampe**
La gestione dello spool delle stampe segue di pari passo la gestione degli utenti/classi utente. Ciascun utente può generare le stampe secondo le abilitazioni definite seguendo i criteri elencati nel presente paragrafo. Come per la gestione utenti, anche per la gestione delle stampe l'Amministratore applicativo ha la possibilità di sovrintendere l'intero sistema delle stampe, per mezzo di funzioni di ricerca mirata all'interno dello spool.

## 8.1.e Protezione dei dati

Anche per la protezione dell'accesso ai dati, il meccanismo si fonda su un sistema di permessi basato sui ruoli definiti in pianta organica e nella gestione utenti descritta al paragrafo precedente. L'accesso ai dati avviene solo attraverso l'applicazione; i server di database sono protetti **da un doppio sistema di firewall e da regole di routing** che non ne consentono la visibilità dall'esterno della rete.
La gestione della base dati unica relativa al singolo Ente è basata su database standard. Nel caso di utilizzo del sistema in modalità Cloud con collegamento al Data Center, il database adottato è Maria DB. In tutti i casi il sistema ne rispecchia le caratteristiche in termini tecnico-funzionali.
I database dei singoli Enti sono distinti e ad ognuno di essi è stato associato un utente/schema. Ad ogni schema non vengono concessi privilegi ulteriori che comportino l'accesso e/o la gestione di oggetti appartenenti ad altri schemi. Non esistono aree condivise tra i vari schemi.
La connessione dall'application server al database avviene attraverso un servizio di rete diverso per ogni Ente. Gli utenti di un ente, al momento dell'accesso, discriminano lo schema associato e l'autenticazione viene effettuata attraverso l'utente, lo schema e relativa password. Questi tre elementi sono indipendenti per ogni ente.

## 8.1.f Tracciabilità dei log di accesso (per eventuali comunicazioni di Data Breach)

Il sistema di autenticazione basato su sessione rende implicitamente disponibile una funzione di monitoraggio attività sul sistema. Attraverso apposita tabella, infatti, possono essere memorizzate le sessioni d'uso istanziate e chiuse, i tentativi di accesso non riusciti, i rinnovi di sessione, ecc. La richiesta al Session Manager, inoltrata ogni qualvolta un utente fa una richiesta a Urbi Smart, WebTec e/o a CDAN, consente di registrare informazioni sulle operazioni eseguite con tracciamento per ogni utente, programma, evento. La logica di base con cui sono sviluppati i programmi di Urbi Smart, WebTec e CDAN fa sì che ciascuna operazione svolta dagli utenti (visualizzazione di una maschera, inserimento, modifica o rimozione di dati) avvenga tramite il richiamo di un evento che viene tracciato. Vengono difatti tracciati:
- token di sessione
- utente loggato
- Remote IP da cui è pervenuta la chiamata
- TimeStamp dell'evento
- estremi della chiamata

La struttura è in grado di memorizzare anche situazioni del tipo:
- "Non si dispone delle credenziali per procedere." @ErroreLogin (dove ErroreLogin riporta l'esatta motivazione dell'errore)
- "Errore in fase di derivazione delle credenziali per la base dati. Chiudere e riaprire il browser, quindi riprovare"
- "Sessione non valida!"
- "Sessione scaduta!"
- "Sessione con IP reimpostato, rieffettuare la login!"
- "Non si dispone delle autorizzazioni per accedere, chiudere il browser e rieffettuare la login!"
- LOGIN utente
- LOGOUT utente.

## 8.1.g Tracciabilità delle variazioni ai dati del sistema

Urbi Smart e WebTec sono dotati di un sistema di monitoraggio delle variazioni alla base dati. Le variazioni applicative alla base dati vengono tracciate riportando, per ogni sessione di variazione:
- grandezza variata
- utente che ha effettuato la variazione
- istanza applicativa che ha provocato la variazione
- valore precedente alla variazione
- valore successivo alla variazione.

Funzioni applicative di interrogazione consentono l'analisi del monitoraggio.

## 9. Erogazione servizio di assistenza remota

PA Digitale fornisce il servizio di assistenza remota attraverso uno specifico settore di Help Desk e mediante due modalità differenti:
1. collegamento da remoto mediante software di accesso a desktop remoto, incluso nel contratto di assistenza;
2. accesso da remoto, tramite l'utente "PAD_SUPPORT" (per il solo Urbi Smart), adottato solo a seguito di sottoscrizione da parte del cliente di una specifica autorizzazione formale.

## 9.1. Collegamento da remoto

Viene utilizzata questa modalità nei casi in cui l'Operatore di Help Desk, per erogare il supporto al cliente richiedente, non abbia la necessità di operare sul sistema del cliente ma solamente di guidare l'Utente e visualizzare le operazioni che quest'ultimo effettua sull'applicativo.
Il collegamento viene effettuato mediante un software di accesso a desktop remoto, leader di mercato, che garantisce la sicurezza degli utenti e delle connessioni mediante infrastruttura certificata ISO/IEC 27001 e interamente conforme alle norme HIPAA e SOC2:
- Crittografia AES a 256 bit
- Autenticazione a due fattori
- Protezione da forza bruta
- Lista bianca per utenti e IP
- Elenco dei dispositivi fidati
- Reset della password forzato.

## 9.2. Accesso mediante utente "PAD_SUPPORT"

A seguito dell'autorizzazione del cliente, predisposta su carta intestata, debitamente sottoscritta e trasmessa via PEC, PA Digitale crea uno specifico utente e provvede alla configurazione dell'ambiente di lavoro.
Per mezzo di questa modalità, abilitata di volta in volta dal Cliente in ciascuna richiesta di assistenza, gli Operatori di Help Desk possono accedere in autonomia al database del cliente tramite uno specifico utente di sistema creato ad hoc (PAD_SUPPORT), al fine effettuare la corretta diagnostica delle problematiche segnalate. Gli Operatori di Help Desk potranno quindi effettuare le operazioni correttive direttamente "sulle" soluzioni applicative in uso dal Cliente - risolvendo dove possibile direttamente le necessità segnalate, senza la necessità che una persona che presidi l'intervento.
Attraverso questa modalità si incrementa l'efficienza dei servizi di Assistenza, velocizzando i tempi di risposta e

procedendo in maniera più rapida alla risoluzione delle problematiche evidenziate, nel rispetto della trasparenza così come della normativa sulla privacy, attraverso una puntuale tracciatura delle attività effettuate dagli Operatori di Help Desk. Tutte le operazioni sono infatti tracciate in uno specifico log che, al termine dell'intervento, viene firmato digitalmente, allegato al ticket di assistenza e messo a disposizione del Cliente nel caso in cui lo richieda.
Nell'eventualità che, per una specifica richiesta d'assistenza, il Cliente non voglia permettere l'utilizzo di tale funzionalità, il richiedente medesimo dovrà disabilitare il check "Assistenza tramite Backdoor in fase di inserimento del ticket", che di base è sempre valorizzato.

## 10. Subappalto di servizi

Nei casi in cui PA Digitale abbia la necessità di subappaltare una componente e/o alcune attività previste dal servizio di utilizzo di Urbi Smart e/o WebTec, dopo aver verificato i requisiti di esperienza, di professionalità, di capacità e di affidabilità del fornitore, sottoscrive con quest'ultimo un contratto formale che contiene, oltre alle clausole contrattuali, il disciplinare tecnico che regolamenta la modalità di erogazione del servizio da prestare e le misure di sicurezza da adottare per garantire la sicurezza delle informazioni e di tutti i dati trattati (con particolare riguardo verso le Informazioni Personali Identificabili - PII).
Nel caso in cui il fornitore, per espletare il proprio servizio, non sia tenuto ad effettuare alcun trattamento di dati personali, tale divieto è espressamente indicato nel contratto di servizio. Nel caso in cui il fornitore debba effettuare un trattamento di dati personali, tale fornitore viene nominato Sub-Responsabile del trattamento dei dati in outsourcing, per ciascun servizio assegnato. Nella lettera di nomina sono riportate:

- le finalità del trattamento
- i dati da trattare
- la base giuridica
- la durata del trattamento
- le indicazioni nonché le specifiche istruzioni a cui attenersi affinché tutte le operazioni di trattamento informatico e manuale dei dati personali, nei limiti delle competenze e attribuzioni del fornitore, siano effettuate nel rispetto della normativa vigente e dei regolamenti aziendali in materia di tutela dei dati personali, prevedendo in particolare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo che il trattamento soddisfi i requisiti del Regolamento UE 2016/679 (art. 28 comma 4).

Non è previsto il subappalto di servizi per l'utilizzo di CDAN.

## 11. La restituzione dei dati a conclusione o revoca del contratto di Urbi Smart e WebTec

All'atto della conclusione e della revoca del contratto in essere, e a seguito del pagamento dell'eventuale debito in essere, PA Digitale in qualità di Responsabile esterno del trattamento:

- permetterà al Titolare del trattamento di prelevare dai sistemi elettronici di PA Digitale gli archivi informatici tramite apposita funzione;
- è tenuta a conservare nell'IDC (Internet Data Center) i dati del Cliente per un periodo non superiore a 90 (novanta) giorni dalla data di cessazione degli Ordinativi di fornitura, per qualsiasi causa essa intervenga. Decorso il suddetto termine, PA Digitale è autorizzata contrattualmente dal Cliente a cancellare fisicamente dall'IDC i dati e tutte le relative copie di salvataggio, con modalità di cancellazione sicura.

Tali misure si applicano ai Clienti che usufruiscano delle soluzioni Urbi Smart e WebTec in Cloud.

## 12. La restituzione dei dati a conclusione o revoca del contratto di Conservazione digitale dei documenti informatici

In caso di risoluzione del Contratto i documenti informatici originariamente versati dal Cliente nel sistema di Conservazione CDAN saranno a quest'ultimo restituiti nel loro formato originale, fatto salvo il caso che i suddetti documenti abbiano subito una conversione di formato per sopperire all'obsolescenza del formato originario; in quest'ultimo caso saranno restituiti nel formato convertito. Contestualmente, saranno restituiti anche i metadati associati ai documenti informatici originariamente forniti dal Cliente.
PA Digitale, in tutti i casi di risoluzione del Contratto, consentirà al Cliente di recuperare i propri documenti informatici, entro e non oltre 90 (novanta) giorni dalla cessazione del Contratto, dopo che questi avrà corrisposto a PA Digitale tutti gli importi contrattualmente dovuti. I documenti informatici dovranno essere prelevati dal Cliente secondo le modalità stabilite nel Manuale del sistema di Conservazione e dal Contratto - quindi non incombe su PA Digitale alcun obbligo di

provvedere alla materiale restituzione dei documenti informatici conservati. Decorso il suddetto termine, PA Digitale è autorizzata contrattualmente dal Cliente a cancellare dal proprio IDC i documenti informatici e gli annessi metadati di cui il Cliente è titolare (e tutte le relative copie di salvataggio), con modalità di cancellazione sicura.