Digitalizzazione della PA e documenti digitali

Benvenuti alla terza lezione del nostro corso sulla digitalizzazione della Pubblica Amministrazione italiana. In questo incontro esploreremo il processo di trasformazione digitale della PA, concentrandoci sui documenti digitali e sugli strumenti che ne garantiscono validità e sicurezza.

Analizzeremo il ruolo fondamentale dell'Agenzia per l'Italia Digitale (AgID) e il Piano Triennale per l'Informatica nella PA, approfondiremo l'importanza dei formati file aperti e studieremo le diverse tipologie di firme digitali. Esamineremo inoltre i sistemi di identità digitale come SPID e CIE, per concludere con un laboratorio pratico sulla creazione e verifica di documenti con firma digitale.

Questa lezione fornirà le competenze essenziali per comprendere e applicare gli strumenti digitali nel contesto della Pubblica Amministrazione italiana.

Agenda della lezione

AgID e Piano Triennale per l'Informatica nella PA

Esploreremo il ruolo dell'Agenzia per l'Italia Digitale e analizzeremo il Piano Triennale come strumento strategico per la digitalizzazione della Pubblica Amministrazione.

Formati file aperti

Approfondiremo le caratteristiche e i vantaggi dei formati aperti nel contesto della PA, evidenziando l'importanza dell'interoperabilità e della conservazione a lungo termine.

Firme digitali

Esamineremo le diverse tipologie di firme elettroniche, il loro valore legale e le tecnologie che ne garantiscono sicurezza e validità nel tempo.

Sistemi di identità digitale

Analizzeremo SPID, CIE e altri sistemi di autenticazione digitale, valutando vantaggi e applicazioni pratiche nella PA.

Protocollo informatico

Esamineremo il sistema di gestione documentale digitale della PA, i suoi requisiti normativi e le modalità di implementazione per garantire validità legale e tracciabilità dei documenti.

AgID: Agenzia per l'Italia Digitale

Definizione e missione

L'Agenzia per l'Italia Digitale (AgID) è l'organismo tecnico del governo italiano che garantisce la realizzazione degli obiettivi dell'Agenda digitale italiana e promuove l'innovazione digitale nel settore pubblico.

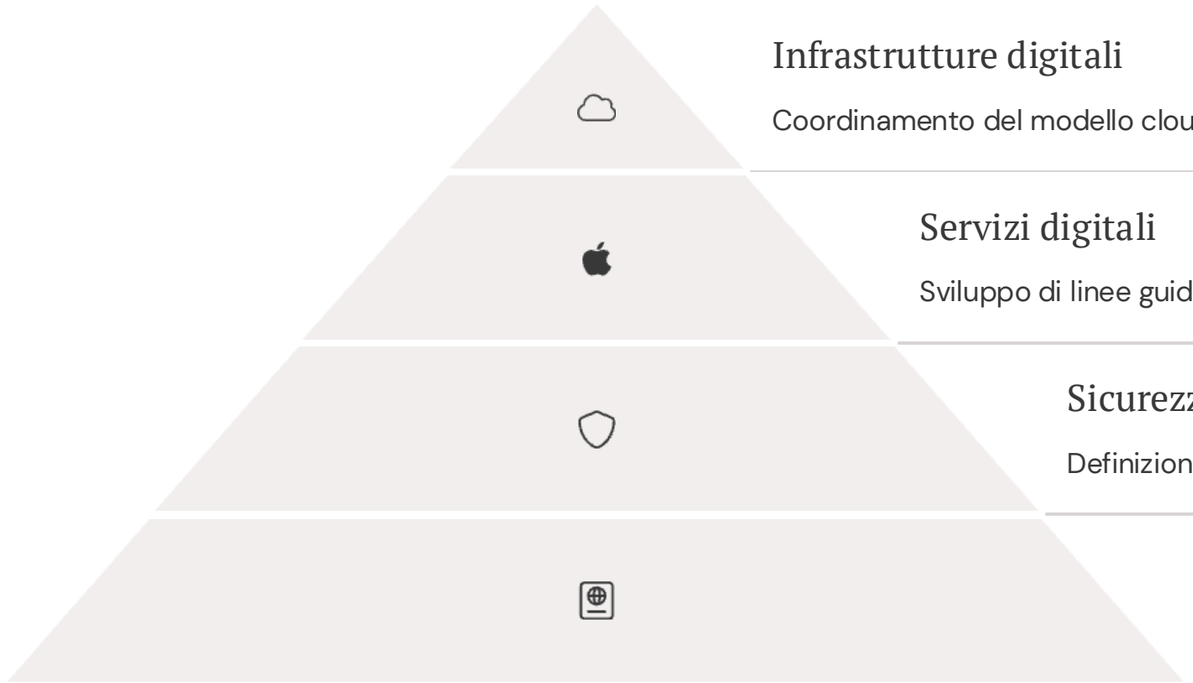
Ruolo normativo

Elabora linee guida, regolamenti e standard tecnici che le amministrazioni pubbliche devono seguire nei processi di digitalizzazione, garantendo uniformità e coerenza a livello nazionale.

Obiettivi strategici

Promuove l'alfabetizzazione digitale, coordina le iniziative di trasformazione digitale, favorisce l'interoperabilità tra i sistemi informatici pubblici e facilita l'accesso ai servizi online per cittadini e imprese.

AgID: principali ambiti di intervento



Infrastrutture digitali

Coordinamento del modello cloud della PA e gestione del Polo Strategico Nazionale

Servizi digitali

Sviluppo di linee guida per app, siti web e servizi digitali pubblici

Sicurezza informatica

Definizione di misure minime di sicurezza e standard di protezione

Protocollo informatico

Gestione documentale digitale, sistema di classificazione e archiviazione dei fascicoli

L'AgID opera come catalizzatore dell'innovazione nel settore pubblico, promuovendo l'adozione di tecnologie sicure ed efficienti. Attraverso la definizione di standard tecnici e architetture di riferimento, garantisce lo sviluppo coordinato delle infrastrutture digitali nazionali.

Nel campo dei servizi digitali, l'Agenzia supporta le amministrazioni nella progettazione di interfacce user-friendly e accessibili, mentre sul fronte della sicurezza informatica svolge un ruolo cruciale nella difesa del patrimonio informativo pubblico e nella protezione dei dati dei cittadini. Per quanto riguarda il protocollo informatico, AgID definisce le regole tecniche per la gestione documentale, la conservazione a norma e l'organizzazione dei fascicoli elettronici.

Piano Triennale per l'Informatica nella PA

Definizione

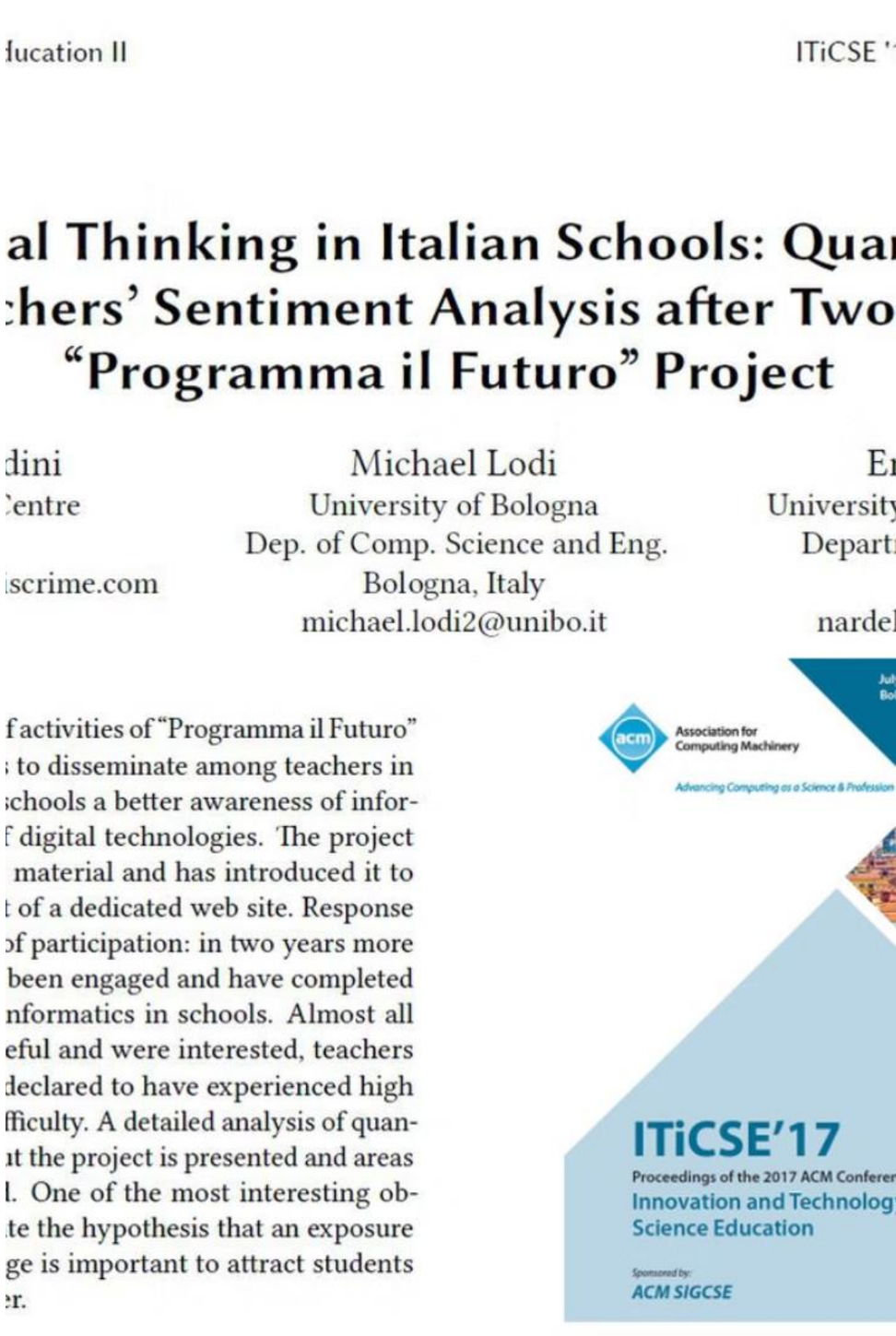
Il Piano Triennale è il documento di indirizzo strategico che guida la trasformazione digitale della Pubblica Amministrazione italiana, definendo obiettivi, priorità e azioni concrete per un periodo di tre anni.

Scopo

Indirizza gli investimenti in tecnologie digitali delle amministrazioni pubbliche secondo priorità condivise, garantendo coerenza a livello nazionale ed evitando duplicazioni o frammentazioni degli interventi.

Evoluzione

Dal primo Piano 2017-2019 all'attuale 2024-2026, il documento ha progressivamente affinato la sua struttura, passando da un approccio principalmente infrastrutturale a uno maggiormente orientato ai servizi e all'esperienza degli utenti.


ducation II ITiCSE '

al Thinking in Italian Schools: Quan
chers' Sentiment Analysis after Two
"Programma il Futuro" Project

dini
Centre
iscrime.com

Michael Lodi
University of Bologna
Dep. of Comp. Science and Eng.
Bologna, Italy
michael.lodi2@unibo.it

Depart
nardel

f activities of "Programma il Futuro"
to disseminate among teachers in
schools a better awareness of infor-
f digital technologies. The project
material and has introduced it to
t of a dedicated web site. Response
of participation: in two years more
been engaged and have completed
nformatics in schools. Almost all
eful and were interested, teachers
declared to have experienced high
fficulty. A detailed analysis of quan-
at the project is presented and areas
l. One of the most interesting ob-
te the hypothesis that an exposure
ge is important to attract students
er.

Association for Computing Machinery
Advancing Computing as a Science & Profession

ITiCSE'17
Proceedings of the 2017 ACM Conferen
Innovation and Technolog
Science Education
Sponsored by:
ACM SIGCSE

Piano Triennale 2024-2026: novità principali

Approccio orientato ai servizi digitali

La nuova edizione del Piano Triennale pone al centro i servizi digitali per cittadini e imprese, superando la precedente focalizzazione sulle infrastrutture. Ogni intervento tecnologico è ora valutato in base al miglioramento tangibile che può portare all'esperienza degli utenti.

- Design dei servizi centrato sull'utente
- Semplificazione delle interfacce
- Misurazione della soddisfazione dell'utente

Focus su governance e monitoraggio

Il Piano 2024-2026 rafforza significativamente gli aspetti di governance e monitoraggio dell'attuazione, introducendo indicatori di performance più dettagliati e meccanismi di verifica continua dei progressi.

- Dashboard di monitoraggio in tempo reale
- Sistemi di alert per ritardi nell'implementazione
- Reportistica strutturata per livelli di responsabilità

Piano Triennale: principi guida

Interoperabilità

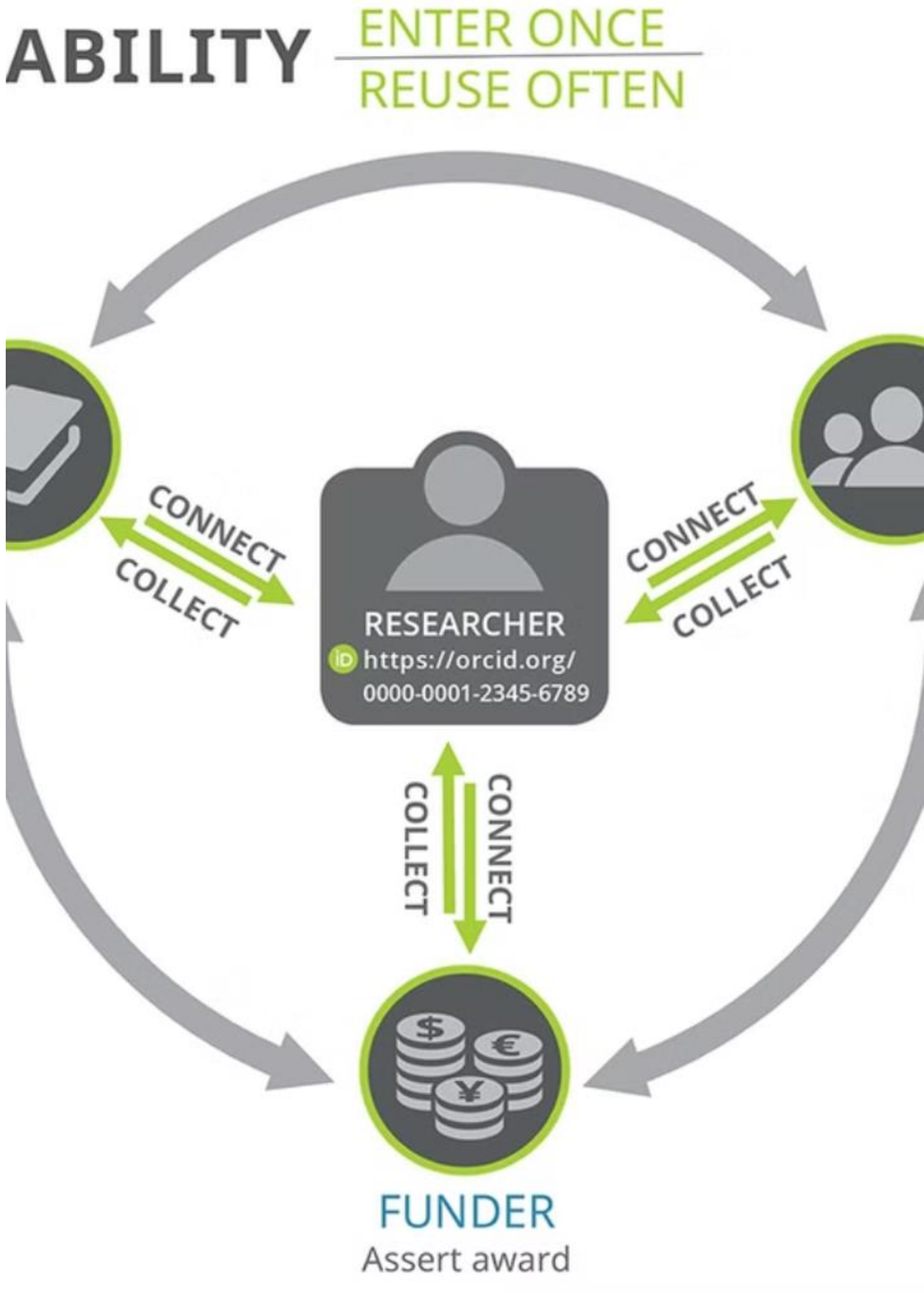
Capacità dei sistemi informatici di scambiarsi informazioni e utilizzare reciprocamente i dati condivisi, superando i "silos informativi" della PA. L'interoperabilità è garantita dall'adozione del Modello di Interoperabilità (ModI) che definisce standard e protocolli comuni.

Once-only

Principio secondo cui cittadini e imprese devono fornire una sola volta le proprie informazioni alla PA, che poi le condividerà internamente. Questo approccio riduce il carico burocratico e migliora l'efficienza amministrativa attraverso la condivisione automatica dei dati.

Cloud first

Priorità all'adozione di soluzioni cloud rispetto a infrastrutture fisiche locali. Questo principio comporta la progressiva migrazione dei servizi digitali della PA verso infrastrutture cloud qualificate, garantendo maggiore efficienza, sicurezza e scalabilità.



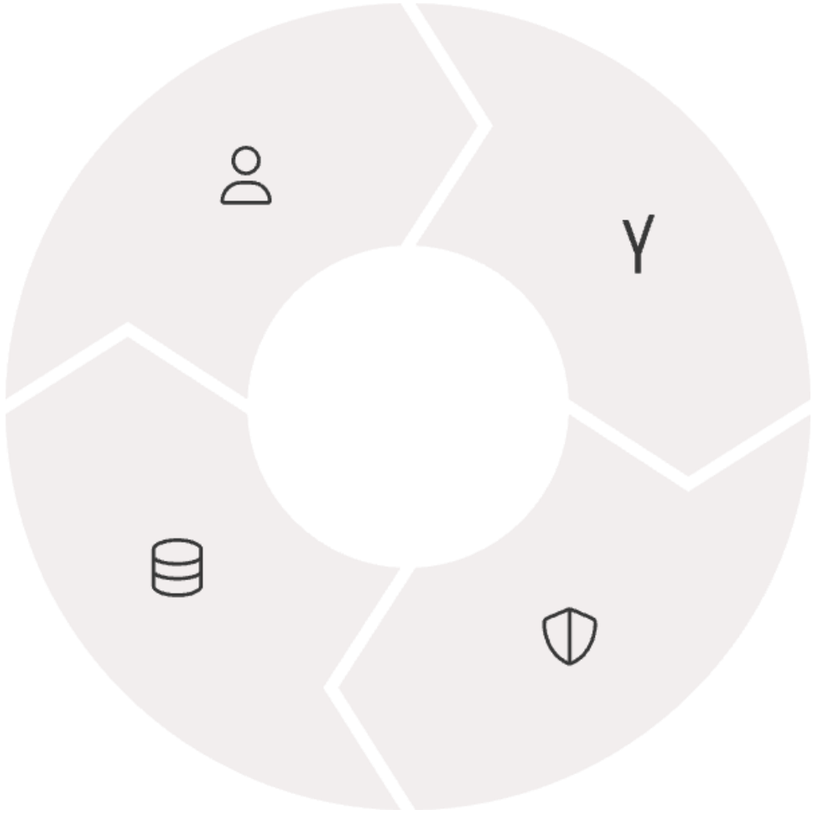
Piano Triennale: obiettivi strategici

Servizi digitali centrati sull'utente

Progettazione di servizi digitali che partono dai bisogni reali di cittadini e imprese

Valorizzazione del patrimonio informativo

Utilizzo strategico dei dati pubblici per migliorare servizi e politiche



Ecosistemi integrati

Creazione di sistemi informativi connessi tra diverse amministrazioni

Infrastrutture sicure e sostenibili

Sviluppo di piattaforme tecnologiche resilienti ed efficienti

Il Piano Triennale mira a ridurre il divario digitale, sia territoriale che demografico, attraverso interventi mirati che garantiscano l'accesso universale ai servizi digitali. Particolare attenzione è dedicata alle aree interne e alle categorie più fragili, con iniziative di formazione e supporto all'utilizzo dei servizi online.

Piano Triennale: azioni chiave

Migrazione al cloud

Il Piano prevede il trasferimento dei servizi digitali delle amministrazioni verso infrastrutture cloud qualificate, secondo il principio Cloud First. Questo processo comporta l'assessment dei sistemi esistenti, la pianificazione della migrazione e la progressiva dismissione dei data center obsoleti.

L'obiettivo è migrare almeno il 75% dei servizi digitali della PA entro il 2026, con priorità per i servizi critici e quelli ad alto impatto per cittadini e imprese.

Potenziamento delle competenze digitali

Un'azione trasversale del Piano riguarda il rafforzamento delle competenze digitali sia dei cittadini che dei dipendenti pubblici. Per questi ultimi, sono previsti programmi strutturati di formazione su tecnologie emergenti, sicurezza informatica e gestione del cambiamento.

L'iniziativa "Repubblica Digitale" coordina gli interventi di alfabetizzazione digitale della popolazione, con l'obiettivo di ridurre il gap rispetto alla media europea.

Intelligenza Artificiale nel Piano Triennale

Linee guida per l'adozione nella PA

Definizione di principi etici e regole tecniche per l'uso dell'IA

Progetti pilota e sperimentazioni

Realizzazione di casi d'uso in ambiti selezionati della PA

Implementazione su vasta scala

Diffusione delle soluzioni validate in tutti gli enti pubblici

Il Piano Triennale 2024-2026 dedica per la prima volta un'attenzione specifica all'Intelligenza Artificiale come leva strategica per modernizzare la Pubblica Amministrazione. Le linee guida sviluppate dall'AgID stabiliscono criteri rigorosi per garantire che l'adozione dell'IA avvenga nel rispetto dei diritti fondamentali dei cittadini, con particolare attenzione alla trasparenza degli algoritmi e alla spiegabilità delle decisioni automatizzate.

Tra le applicazioni più promettenti dell'IA nella PA italiana figurano i sistemi di assistenza virtuale ai cittadini, l'ottimizzazione dei processi interni e l'analisi predittiva per la pianificazione dei servizi pubblici. Tutti gli utilizzi devono comunque prevedere sempre la supervisione umana sulle decisioni rilevanti.

Strumenti operativi del Piano Triennale

Modelli di supporto

Il Piano Triennale fornisce alle amministrazioni una serie di modelli documentali standardizzati per facilitare la pianificazione degli interventi di digitalizzazione. Questi template coprono diverse fasi del processo:

- Assessment della maturità digitale
- Analisi costi-benefici per la migrazione al cloud
- Piani di formazione per il personale
- Documentazione tecnica per l'interoperabilità

I modelli sono disponibili sul portale di AgID e vengono aggiornati periodicamente per riflettere le evoluzioni tecnologiche e normative.

Check-list per la pianificazione

Per agevolare le amministrazioni nell'implementazione del Piano, sono state sviluppate check-list operative che guidano passo dopo passo gli enti pubblici nelle attività di pianificazione:

- Verifica di conformità normativa
- Controllo dei requisiti di sicurezza
- Valutazione dell'accessibilità dei servizi
- Monitoraggio dell'avanzamento delle attività

Queste check-list permettono anche di identificare rapidamente eventuali criticità e attivare le necessarie azioni correttive.

Monitoraggio del Piano Triennale

42	3	4
Indicatori chiave	Livelli di monitoraggio	Report trimestrali
Metriche quantitative utilizzate per misurare i progressi	Strategico, direzionale e operativo	Frequenza della verifica formale dei progressi

Il sistema di monitoraggio del Piano Triennale si basa su una piattaforma digitale centralizzata che raccoglie automaticamente i dati dalle amministrazioni e li elabora per produrre indicatori sintetici sull'avanzamento delle diverse linee d'azione. Gli indicatori di performance riguardano sia aspetti quantitativi (numero di servizi migrati al cloud, percentuale di dipendenti formati) sia qualitativi (usabilità dei servizi, soddisfazione degli utenti).

I meccanismi di verifica prevedono controlli documentali, audit tecnici presso le amministrazioni e, per la prima volta, l'utilizzo di test automatizzati che verificano in tempo reale la conformità dei servizi digitali agli standard definiti. I risultati del monitoraggio sono pubblicati sul portale dedicato, garantendo trasparenza verso cittadini e stakeholder.

Formati file: definizione e importanza

Cosa sono i formati file

I formati file sono convenzioni standardizzate che definiscono come le informazioni vengono codificate, memorizzate e organizzate all'interno di un file digitale. Ogni formato ha caratteristiche specifiche che lo rendono adatto a particolari tipi di contenuti (testi, immagini, audio, video) e utilizzi.

I formati file determinano non solo come i dati sono archiviati, ma anche quali software possono leggerli e modificarli, influenzando direttamente l'accessibilità e la longevità delle informazioni digitali.

Rilevanza per la PA digitale

Nella Pubblica Amministrazione, la scelta dei formati file assume importanza strategica per diverse ragioni:

- Garantisce l'accesso ai documenti nel lungo periodo
- Facilita lo scambio di informazioni tra enti diversi
- Assicura la correttezza e l'integrità dei dati
- Promuove la trasparenza amministrativa
- Riduce i costi di gestione e manutenzione

La normativa italiana impone alle PA l'utilizzo preferenziale di formati aperti per evitare vincoli tecnologici e garantire la sovranità digitale.

Formati file aperti vs proprietari

Formati aperti

- Specifiche tecniche pubbliche e accessibili
- Sviluppati da comunità o consorzi con processi trasparenti
- Utilizzo libero senza restrizioni legali o economiche
- Indipendenti da specifici software o piattaforme
- Esempi: PDF/A, ODF, HTML, CSV, XML

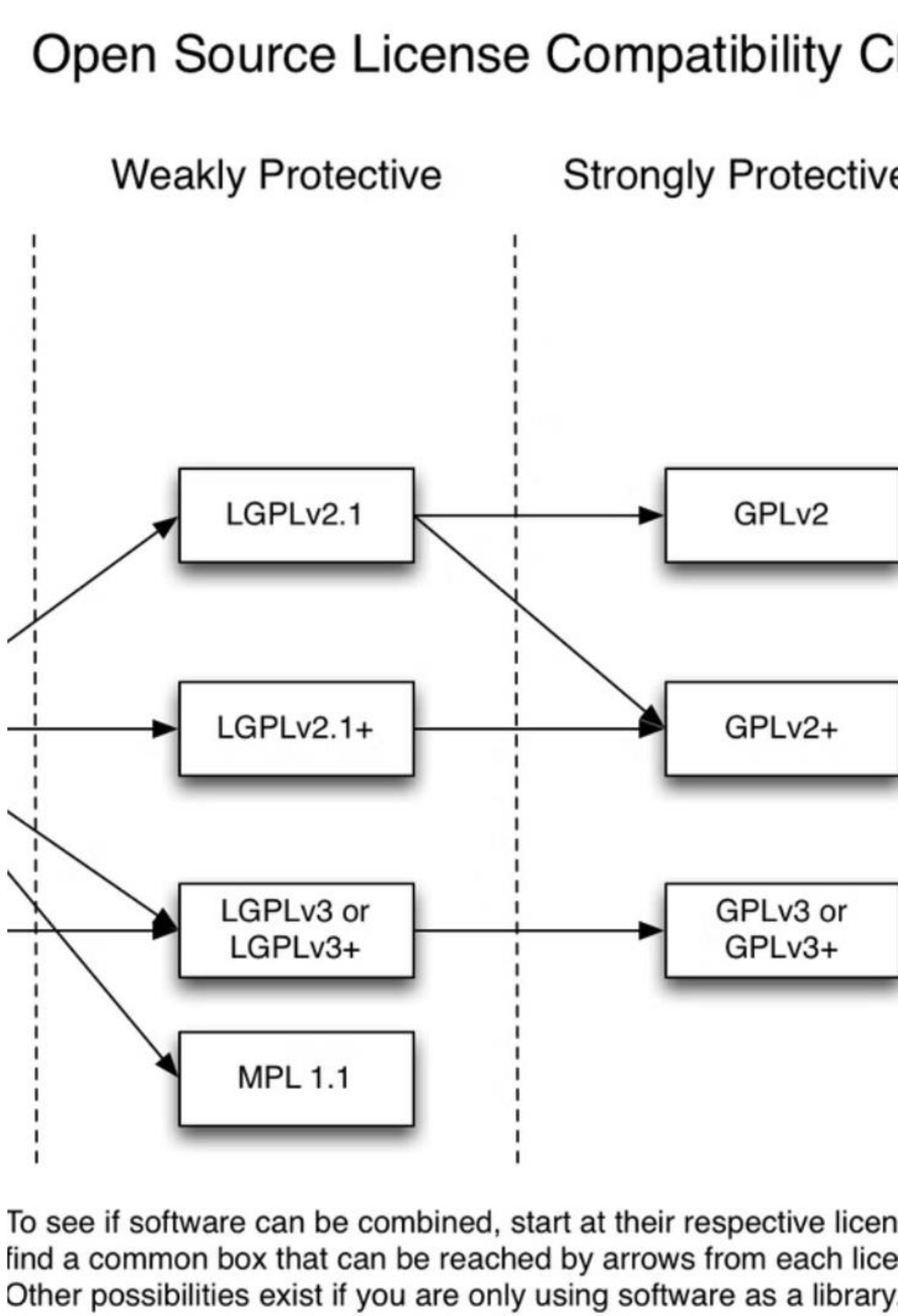
Formati proprietari

- Specifiche tecniche riservate o parzialmente accessibili
- Sviluppati e controllati da singole aziende
- Spesso soggetti a licenze o brevetti limitanti
- Generalmente legati a specifici software commerciali
- Esempi: DOC, XLS, PSD, DWG

Valutazione comparativa

I formati aperti garantiscono maggiore interoperabilità, accessibilità a lungo termine e indipendenza dai fornitori, ma possono talvolta offrire funzionalità più limitate rispetto ai formati proprietari.

I formati proprietari spesso offrono funzionalità avanzate e ottimizzate, ma creano dipendenza dai fornitori e possono presentare problemi di compatibilità futura.



Caratteristiche dei formati aperti

Specifiche pubbliche

Le caratteristiche tecniche del formato sono completamente documentate e accessibili a chiunque, permettendo a sviluppatori indipendenti di creare software in grado di leggere e produrre file in quel formato senza restrizioni.

Assenza di restrizioni legali

Il formato può essere utilizzato liberamente senza dover corrispondere royalty o affrontare limitazioni brevettuali. Questo permette a qualsiasi soggetto, pubblico o privato, di implementare il formato nei propri sistemi senza costi aggiuntivi o vincoli contrattuali.

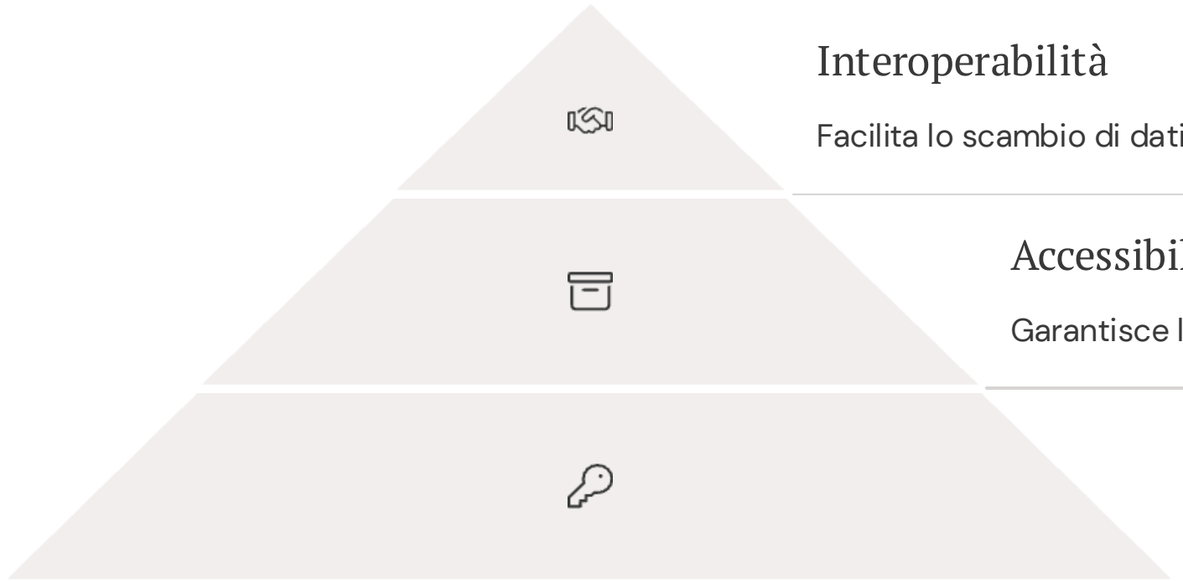
Gestione indipendente

Il formato è sviluppato, mantenuto e aggiornato da organizzazioni non profit, consorzi industriali aperti o enti di standardizzazione, garantendo che l'evoluzione del formato risponda alle esigenze della comunità piuttosto che agli interessi commerciali di una singola azienda.

Stabilità e retrocompatibilità

I formati aperti tendono a mantenere la compatibilità con le versioni precedenti, permettendo l'accesso ai dati anche quando il software evolve, proteggendo così gli investimenti e preservando il valore dell'informazione nel tempo.

Vantaggi dei formati aperti



Interoperabilità

Facilita lo scambio di dati tra enti e sistemi diversi

Accessibilità a lungo termine

Garantisce l'accesso futuro ai documenti indipendentemente dall'evoluzione tecnologica

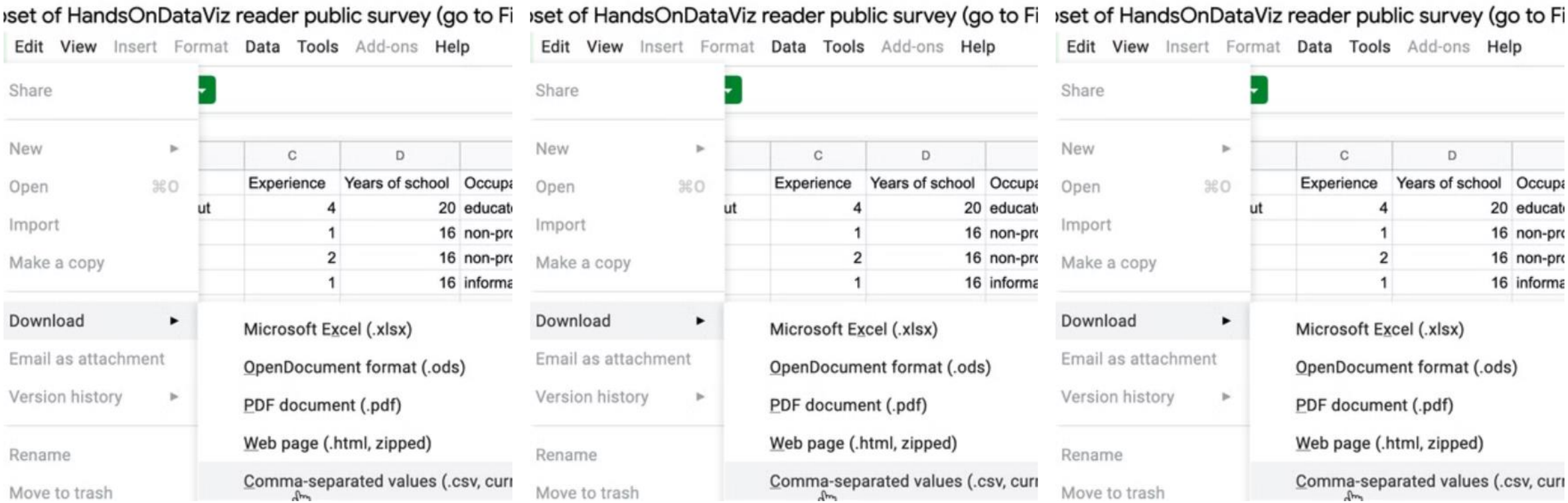
Riduzione del vendor lock-in

Elimina la dipendenza da specifici fornitori di software o servizi

L'interoperabilità garantita dai formati aperti permette alla Pubblica Amministrazione di scambiare dati e documenti senza barriere tecnologiche, facilitando la collaborazione tra enti diversi e l'integrazione dei servizi. Questo si traduce in processi amministrativi più efficienti e in una migliore esperienza per cittadini e imprese.

La conservazione a lungo termine è un aspetto cruciale per le PA, che hanno l'obbligo di garantire l'accesso ai documenti amministrativi per periodi estesi, talvolta decenni. I formati aperti, grazie alla documentazione pubblica delle loro specifiche, assicurano che i documenti rimangano leggibili anche quando le applicazioni originali con cui sono stati creati non sono più disponibili.

Formati aperti comuni: CSV



Il CSV (Comma-Separated Values) è un formato semplice e universale per la rappresentazione di dati tabulari. Ogni riga del file corrisponde a un record, mentre i valori all'interno di ciascuna riga sono separati da virgole o altri delimitatori. La sua semplicità strutturale lo rende ideale per lo scambio di grandi quantità di dati tra sistemi diversi.

Nella Pubblica Amministrazione italiana, il CSV è ampiamente utilizzato per la pubblicazione di dataset aperti su portali come dati.gov.it. Esempi tipici includono elenchi di strutture pubbliche, dati statistici, bilanci in formato aperto e registri amministrativi. La semplicità del CSV facilita l'analisi e l'elaborazione dei dati da parte di cittadini, ricercatori e imprese, promuovendo trasparenza e partecipazione.

Formati aperti comuni: JSON

2001	2	6
Anno di creazione	Strutture di base	Tipi di dati supportati
Sviluppato da Douglas Crockford	Oggetti e array per organizzare i dati	Stringhe, numeri, booleani, null, oggetti e array

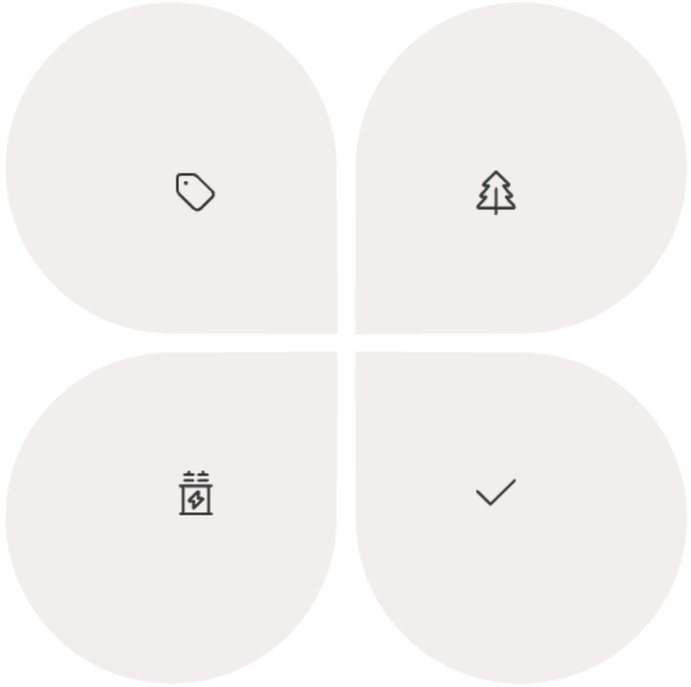
JSON (JavaScript Object Notation) è un formato leggero per lo scambio di dati, facile da leggere e scrivere per gli esseri umani e semplice da analizzare e generare per le macchine. La sua struttura gerarchica e flessibile lo rende particolarmente adatto per rappresentare informazioni complesse e relazionali.

Nella PA digitale italiana, JSON viene utilizzato principalmente nelle API (Application Programming Interfaces) che permettono l'interoperabilità tra sistemi diversi. È il formato prediletto per i servizi web moderni e per l'implementazione del Modello di Interoperabilità delle PA. Applicazioni concrete includono lo scambio di dati tra enti diversi nell'Anagrafe Nazionale della Popolazione Residente (ANPR) e nel Fascicolo Sanitario Elettronico (FSE).

Formati aperti comuni: XML

Struttura a tag

XML utilizza elementi delimitati da tag di apertura e chiusura, simili all'HTML ma personalizzabili



Organizzazione gerarchica

I dati sono organizzati in una struttura ad albero con elementi annidati che rappresentano relazioni padre-figlio

Trasformabilità

Attraverso XSLT, i documenti XML possono essere convertiti in altri formati come HTML o PDF

Schema di validazione

XML supporta DTD e XML Schema per definire regole strutturali e validare i documenti

XML (eXtensible Markup Language) è un formato versatile che permette di definire linguaggi di markup personalizzati per rappresentare strutture dati complesse. La sua ricchezza semantica e gli strumenti di validazione lo rendono ideale per documenti che richiedono integrità strutturale e relazioni complesse tra i dati.

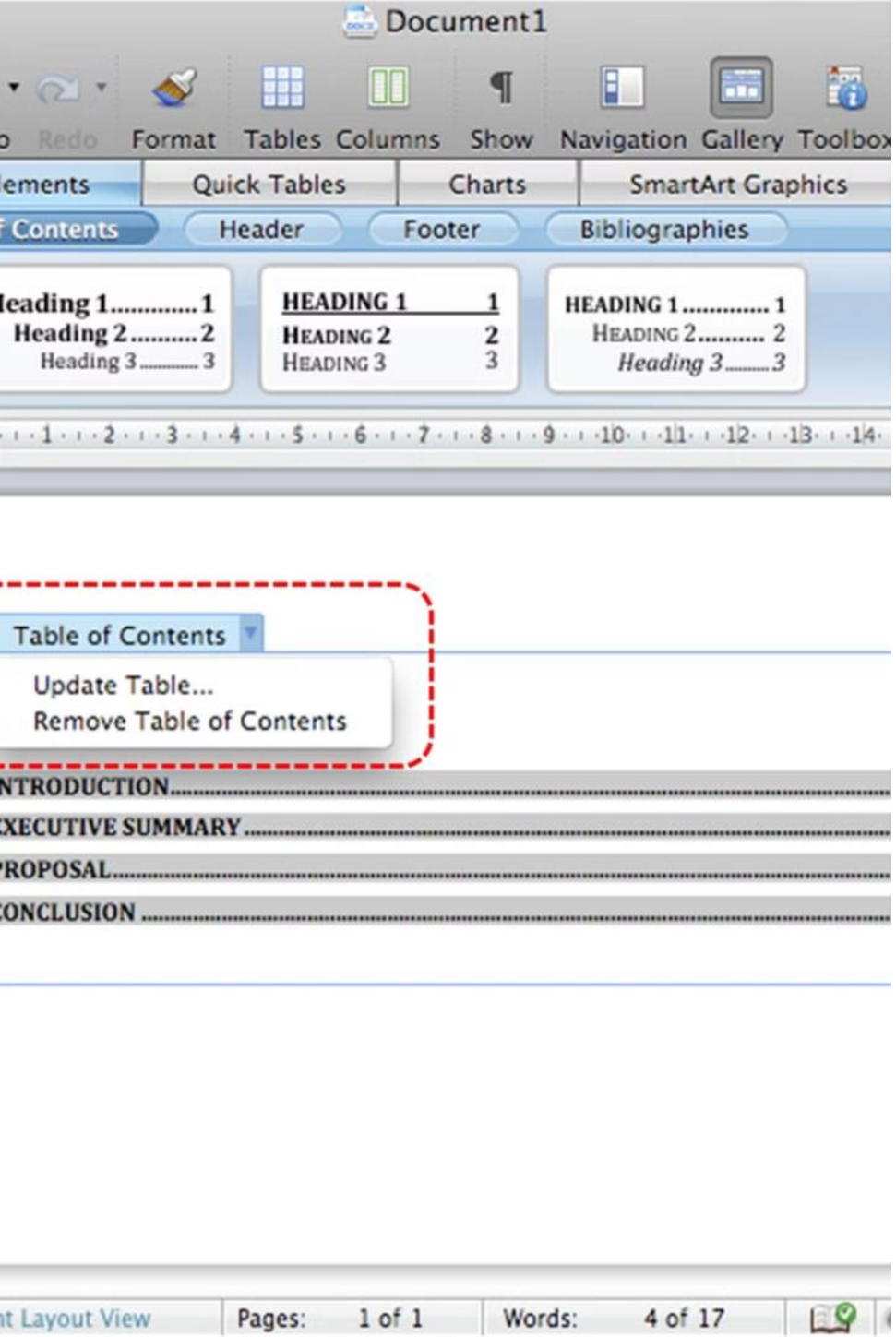
Nella PA italiana, XML è utilizzato in numerosi contesti: dalla fatturazione elettronica (formato FatturaPA) ai documenti di gara (formato DGUE), dai documenti sanitari (standard HL7) alle comunicazioni con il sistema giudiziario. La sua flessibilità permette di rappresentare documenti amministrativi complessi mantenendo la validità formale e l'interoperabilità tra sistemi diversi.

Formati aperti per i dati: Parquet, ORC, Avro

Formato	Caratteristiche principali	Vantaggi nella PA
Parquet	Formato colonnare, ottimizzato per query analitiche	Elaborazione efficiente di grandi dataset statistici
ORC	Ottimizzato per Hadoop, supporta indici e compressione avanzata	Analisi di serie storiche di dati amministrativi
Avro	Schema basato su JSON, ottimo per dati in evoluzione	Gestione di flussi di dati da sistemi diversi

Questi formati avanzati sono progettati specificamente per l'analisi di grandi volumi di dati (Big Data) e si distinguono dai formati tradizionali per le loro prestazioni superiori in contesti di elaborazione distribuita. Utilizzano tecniche sofisticate di compressione, indicizzazione e organizzazione dei dati che riducono significativamente lo spazio di archiviazione e accelerano i tempi di query.

Nella Pubblica Amministrazione italiana, l'adozione di questi formati sta crescendo nell'ambito di progetti di data analytics e intelligenza artificiale. L'ISTAT, ad esempio, utilizza Parquet per l'elaborazione di dati censuari, mentre l'Agenzia delle Entrate sta sperimentando ORC per l'analisi dei dati fiscali. Questi formati permettono alle PA di gestire efficacemente la crescente mole di dati generati dai servizi digitali.



Scelta del formato aperto adeguato

Identificare lo scopo del documento

- Pubblicazione e diffusione (PDF/A, HTML)
- Elaborazione e modifica (ODF, CSV, JSON)
- Preservazione a lungo termine (PDF/A, XML)
- Scambio dati tra sistemi (JSON, XML)

Valutare requisiti tecnici

- Dimensione prevista dei dati
- Complessità della struttura
- Necessità di validazione formale
- Frequenza di aggiornamento

Considerare i destinatari

- Competenze tecniche degli utenti
- Software tipicamente utilizzati
- Accessibilità per persone con disabilità
- Facilità di riutilizzo dei dati

Verificare conformità normativa

- Rispetto delle linee guida AgID
- Aderenza al CAD
- Compatibilità con standard europei
- Requisiti di accessibilità (legge Stanca)

Normativa sui formati aperti

1 Codice dell'Amministrazione Digitale (D.Lgs. 82/2005)

L'articolo 68 stabilisce che le pubbliche amministrazioni devono privilegiare l'adozione di formati aperti nell'acquisizione e nella realizzazione di programmi informatici. Definisce inoltre i requisiti che un formato deve soddisfare per essere considerato aperto.

2 Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici (2021)

Specificano i formati idonei per la formazione e conservazione di documenti digitali, distinguendo tra formati aperti, proprietari e standard. Forniscono criteri di scelta e tabelle comparative per guidare le amministrazioni.

3 Piano Triennale per l'Informatica nella PA

Ribadisce l'importanza dei formati aperti per garantire l'interoperabilità e prevede azioni specifiche per promuoverne l'adozione. Definisce roadmap e indicatori di monitoraggio per valutare i progressi nell'utilizzo di formati aperti.

Firme digitali: introduzione

Definizione e scopo

La firma digitale è un particolare tipo di firma elettronica qualificata che permette di garantire l'autenticità, l'integrità e il non ripudio di un documento informatico. Si basa su un sistema di chiavi crittografiche asimmetriche, una pubblica e una privata, correlate tra loro.

Lo scopo principale della firma digitale è equiparare giuridicamente i documenti informatici a quelli cartacei firmati a mano, permettendo così la completa dematerializzazione dei processi amministrativi e contrattuali.

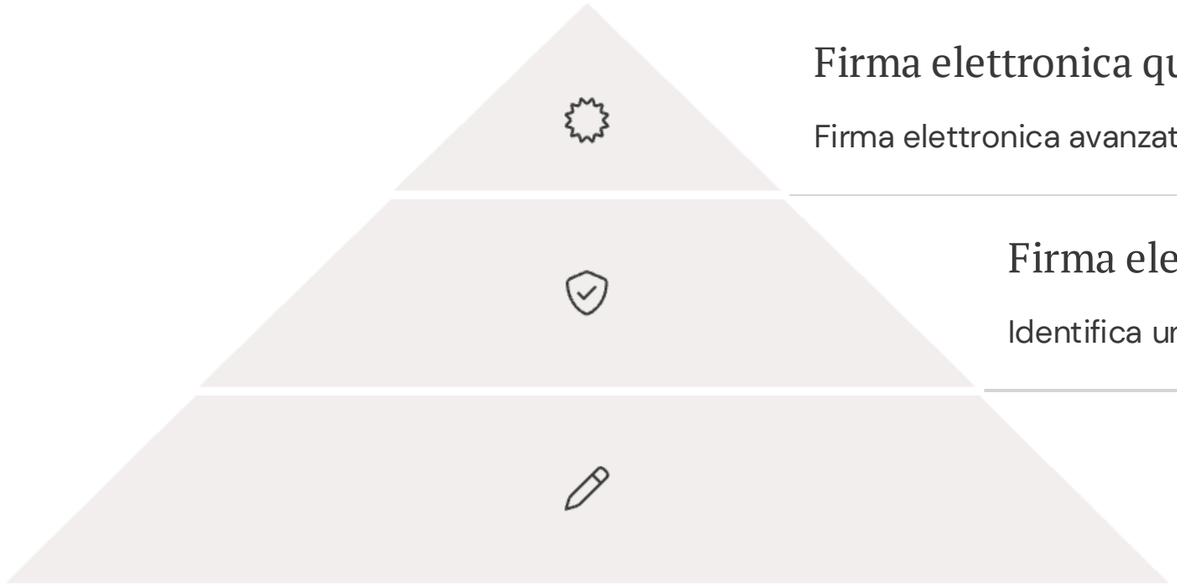
Quadro normativo di riferimento

In Italia, la firma digitale è regolamentata da diversi testi normativi che ne definiscono le caratteristiche tecniche, i requisiti e il valore legale:

- Codice dell'Amministrazione Digitale (D.Lgs. 82/2005, artt. 20-24)
- Regolamento eIDAS (Reg. UE 910/2014)
- DPCM 22 febbraio 2013 (regole tecniche)
- Linee Guida AgID sulla firma digitale

Questo corpus normativo stabilisce i requisiti di sicurezza, le modalità di verifica e i soggetti abilitati al rilascio dei certificati di firma.

Tipologie di firme elettroniche



Firma elettronica qualificata

Firma elettronica avanzata basata su certificato qualificato

Firma elettronica avanzata

Identifica univocamente il firmatario con elevato livello di sicurezza

Firma elettronica semplice

Dati in forma elettronica connessi logicamente ad altri dati

La **firma elettronica semplice** è la tipologia più basilare e può consistere in credenziali di accesso, PIN, password o anche nella scansione di una firma autografa. Ha un valore probatorio limitato e la sua validità può essere facilmente contestata in sede legale.

La **firma elettronica avanzata (FEA)** offre un livello superiore di sicurezza, garantendo l'identificazione del firmatario e l'integrità del documento. Esempi includono la firma grafometrica su tablet e i sistemi di firma OTP (One-Time Password). La FEA è accettata per molti atti, tranne quelli che richiedono forma scritta a pena di nullità.

La **firma elettronica qualificata (FEQ)**, di cui la firma digitale è il principale esempio in Italia, offre il massimo livello di sicurezza ed è l'unica pienamente equiparata alla firma autografa per tutti gli atti. Si basa su certificati qualificati rilasciati da prestatori di servizi fiduciari accreditati.

Firma digitale: caratteristiche tecniche

Crittografia asimmetrica

La firma digitale si basa su una coppia di chiavi crittografiche asimmetriche: una chiave privata, nota solo al titolare e utilizzata per firmare i documenti, e una chiave pubblica, distribuita liberamente e utilizzata per verificare l'autenticità della firma. Le due chiavi sono matematicamente correlate, ma è computazionalmente impossibile ricavare la chiave privata conoscendo quella pubblica.

Funzioni di hash

Prima della firma, il documento viene elaborato attraverso una funzione crittografica di hash che ne produce un'impronta digitale (digest) di lunghezza fissa. Questa impronta è unica per ogni documento e anche la minima modifica al contenuto produrrebbe un'impronta completamente diversa. L'algoritmo più utilizzato attualmente è SHA-256, che genera digest di 256 bit.

Dispositivi sicuri

La chiave privata è custodita in dispositivi sicuri che ne impediscono l'estrazione o la duplicazione. Questi dispositivi possono essere fisici (smart card, token USB) o virtuali (HSM - Hardware Security Module). L'accesso alla chiave privata è protetto da credenziali personali (PIN o password) conosciute solo dal titolare.

Validità legale delle firme digitali

Equiparazione alla firma autografa

Secondo l'art. 24 del CAD, la firma digitale ha la stessa validità legale della firma autografa tradizionale. Questo significa che un documento informatico sottoscritto con firma digitale soddisfa il requisito della forma scritta e ha l'efficacia della scrittura privata prevista dall'art. 2702 del Codice Civile, facendo piena prova della provenienza delle dichiarazioni.

Valore probatorio in giudizio

I documenti informatici con firma digitale sono ammissibili come prova in giudizio. In caso di contestazione, l'onere della prova ricade sulla parte che contesta l'autenticità della firma, invertendo così il normale onere probatorio. La validità temporale della firma è garantita dal riferimento temporale o dalla marca temporale associata.

Casi d'uso nella PA

La firma digitale è obbligatoria per numerosi atti della Pubblica Amministrazione, come contratti pubblici, determine dirigenziali, delibere, fatture elettroniche e documenti del fascicolo sanitario elettronico. È inoltre essenziale per la partecipazione a gare d'appalto e per l'invio di pratiche telematiche a enti pubblici tramite PEC.

Processo di firma digitale

Creazione dell'impronta

Il documento viene elaborato attraverso un algoritmo di hash (tipicamente SHA-256) che ne produce un'impronta digitale univoca. Questa impronta rappresenta sinteticamente il contenuto del documento ed è significativamente più piccola del documento originale.

Cifratura dell'impronta

L'impronta digitale viene cifrata utilizzando la chiave privata del firmatario. Questa operazione può essere eseguita solo dal possessore legittimo della chiave privata, garantendo così l'autenticità della firma.

Generazione della firma

La firma digitale vera e propria consiste nell'impronta cifrata insieme ai metadati che identificano il firmatario (riferimenti al certificato) e alle informazioni temporali.

Incorporazione nel documento

La firma digitale viene incorporata nel documento elettronico o allegata ad esso. Nel caso dei PDF, la firma può essere visibile (con un'immagine grafica) o invisibile (solo a livello tecnico).

Verifica della firma digitale

Estrazione del certificato

Dal documento firmato viene estratto il certificato digitale che contiene la chiave pubblica del firmatario e le informazioni sulla sua identità

Decifratura della firma

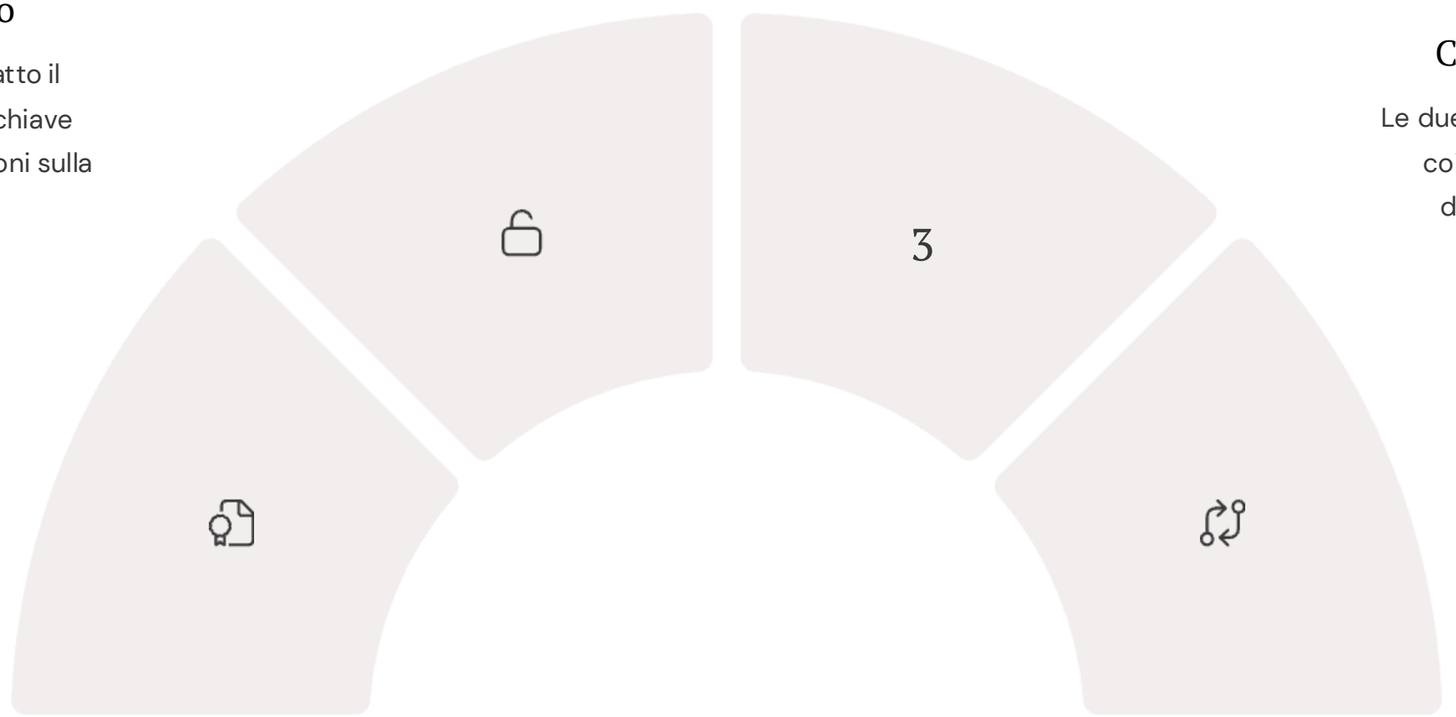
La firma digitale viene decifrata utilizzando la chiave pubblica del firmatario, ottenendo l'impronta originale del documento

Ricalcolo dell'impronta

Viene calcolata nuovamente l'impronta del documento utilizzando lo stesso algoritmo di hash

Confronto delle impronte

Le due impronte vengono confrontate: se coincidono, la firma è autentica e il documento non è stato alterato



Il processo di verifica include anche controlli aggiuntivi sulla validità del certificato, come la verifica che non sia scaduto o revocato. Questa verifica avviene consultando le Certificate Revocation List (CRL) o utilizzando il protocollo OCSP (Online Certificate Status Protocol) che controlla in tempo reale lo stato del certificato presso l'autorità di certificazione.

Per facilitare la verifica delle firme digitali, sono disponibili diversi strumenti sia desktop che online. In Italia, AgID fornisce un verificatore ufficiale chiamato "Digital Signature Verification" (DSV) che permette di controllare l'autenticità e la validità di firme e certificati secondo la normativa italiana ed europea.

Marca temporale

Definizione e funzione

La marca temporale (timestamp) è una sequenza di caratteri che rappresenta una data e un'ora associata a un documento informatico. La sua funzione principale è attestare l'esistenza di un documento in un determinato momento temporale, consentendo così di "cristallizzare" nel tempo il contenuto del documento e la sua firma.

A differenza di un semplice riferimento temporale (come la data del sistema), la marca temporale è rilasciata da un certificatore accreditato (Time Stamping Authority - TSA) e ha valore legale, grazie all'utilizzo di protocolli crittografici che ne garantiscono l'autenticità e l'integrità.

Integrazione con la firma digitale

La marca temporale è particolarmente importante quando viene associata a una firma digitale, poiché permette di:

- Estendere la validità della firma oltre la scadenza del certificato
- Dimostrare che la firma è stata apposta quando il certificato era ancora valido
- Stabilire con certezza l'ordine cronologico di più firme su uno stesso documento
- Fornire evidenza temporale in caso di controversie legali

Il processo di apposizione di firma digitale con marca temporale è chiamato "firma digitale con riferimento temporale opponibile a terzi" ed è spesso richiesto per documenti di particolare rilevanza legale o destinati alla conservazione a lungo termine.

Firme digitali remote

Caratteristiche

Le firme digitali remote sono un'evoluzione delle firme digitali tradizionali in cui la chiave privata del firmatario non è conservata su un dispositivo fisico in suo possesso (smart card o token USB), ma è custodita da un certificatore qualificato su Hardware Security Module (HSM) remoti ad alta sicurezza.

L'accesso alla chiave privata avviene tramite sistemi di autenticazione forte, tipicamente multifattore, che possono includere password, codici OTP (One-Time Password) inviati via SMS o generati da app, o addirittura sistemi biometrici.

Vantaggi

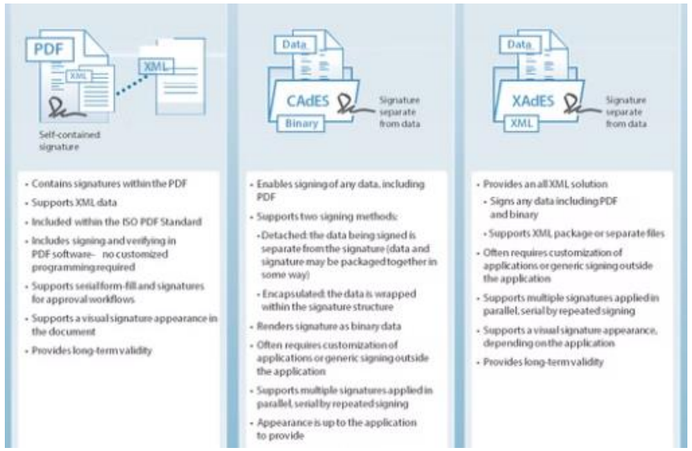
- Eliminazione della necessità di dispositivi fisici e lettori hardware
- Accessibilità da qualsiasi dispositivo connesso a internet
- Possibilità di firmare documenti anche in mobilità
- Maggiore facilità per le firme multiple e i flussi di approvazione
- Riduzione dei costi di gestione e manutenzione

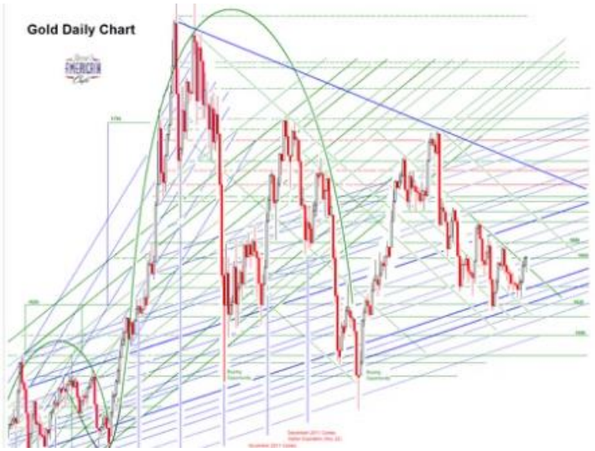
Implementazione nella PA

Nella Pubblica Amministrazione italiana, le firme remote stanno progressivamente sostituendo i sistemi tradizionali grazie alla loro praticità e scalabilità. Vengono utilizzate per la firma di atti amministrativi, delibere, contratti pubblici e comunicazioni ufficiali.

Progetti come "Firma con CIE" permettono ai cittadini di firmare documenti digitali utilizzando la propria Carta d'Identità Elettronica come strumento di autenticazione per accedere a servizi di firma remota, semplificando ulteriormente l'interazione digitale con la PA.

PAdES: firma PDF





PAdES (PDF Advanced Electronic Signatures) è un insieme di standard tecnici che definiscono come implementare firme elettroniche avanzate all'interno di documenti PDF. Basato sullo standard ISO 32000, PAdES è stato sviluppato specificamente per garantire la validità legale e l'interoperabilità delle firme digitali nei documenti PDF, formato ampiamente utilizzato per la documentazione ufficiale.

Le firme PAdES presentano numerosi vantaggi per la Pubblica Amministrazione: permettono di visualizzare il documento firmato con qualsiasi lettore PDF standard, supportano sia firme visibili (con rappresentazione grafica) che invisibili, consentono firme multiple sullo stesso documento, e includono automaticamente l'intero percorso di certificazione. Inoltre, lo standard PAdES Long Term (PAdES-LTV) integra tutti gli elementi necessari per la verifica a lungo termine della firma, inclusi certificati, CRL e marche temporali.

XAdES: firma XML

XAdES Base

Implementazione base dello standard con elementi essenziali di firma

XAdES-T

Aggiunge marca temporale per garantire validità nel tempo

XAdES-A

Supporta archivio di validazione per conservazione a lungo termine

XAdES (XML Advanced Electronic Signatures) è lo standard europeo per le firme digitali applicate a documenti XML. Si basa sullo standard XMLDSig del W3C, estendendolo per garantire la conformità ai requisiti legali europei. A differenza di PAdES, che è specifico per i PDF, XAdES può essere applicato a qualsiasi contenuto XML e supporta diversi "profili" con livelli crescenti di garanzia e longevità.

Nella Pubblica Amministrazione italiana, XAdES viene ampiamente utilizzato per documenti strutturati che richiedono elaborazione automatica e interoperabilità tra sistemi. Applicazioni tipiche includono la fatturazione elettronica (formato FatturaPA), i documenti di gara in formato XML, le dichiarazioni fiscali telematiche e lo scambio di informazioni tra sistemi informativi pubblici. La natura strutturata di XML permette non solo di firmare l'intero documento, ma anche specifiche sezioni o elementi, offrendo maggiore flessibilità in scenari complessi.

CAdES: firma per qualsiasi file

Compatibilità universale

Applicabile a qualsiasi formato di file digitale

Struttura a busta

Incapsula il documento originale preservandone l'integrità

Robustezza crittografica

Implementa algoritmi di sicurezza avanzati e verificabili

Estensioni temporali

Supporta marche temporali e meccanismi di validità estesa

CAdES (CMS Advanced Electronic Signatures) è uno standard per firme digitali basato sul formato CMS (Cryptographic Message Syntax) definito da IETF. La sua caratteristica principale è la versatilità: mentre PAdES è specifico per i PDF e XAdES per i documenti XML, CAdES può essere applicato a qualsiasi tipo di file digitale, mantenendo il formato originale inalterato.

Nella PA digitale, CAdES viene utilizzato quando è necessario firmare tipologie di file per cui non esistono standard specifici o quando si deve preservare il formato originale del documento. Esempi tipici includono la firma di documenti tecnici (CAD, GIS), file multimediali, archivi compressi o formati proprietari. Il file risultante ha tipicamente estensione .p7m e richiede software specifici per la visualizzazione e la verifica, ma garantisce la massima compatibilità indipendentemente dal contenuto.

Conservazione a norma dei documenti firmati

Verifica iniziale

Controllo dell'integrità e della validità di firme e marche temporali

Archiviazione sicura

Memorizzazione in sistemi ridondanti con backup regolari

Metadatazione

Aggiunta di metadati descrittivi e di contesto

Refreshing ciclico

Aggiornamento periodico delle firme e delle marche temporali

La conservazione a norma è il processo che garantisce l'autenticità, l'integrità, l'affidabilità, la leggibilità e la reperibilità dei documenti informatici nel tempo, in conformità con la normativa vigente. Per i documenti firmati digitalmente, questo processo è particolarmente cruciale poiché le firme digitali hanno una validità limitata legata alla scadenza dei certificati.

La Pubblica Amministrazione è obbligata a conservare i propri documenti informatici seguendo le Linee Guida AgID sulla conservazione. Il processo deve essere gestito da un Responsabile della Conservazione e può essere svolto internamente o affidato a conservatori accreditati. Le best practices includono l'applicazione di marche temporali prima della scadenza dei certificati, l'adozione di formati aperti per la conservazione a lungo termine, e l'implementazione di processi regolari di verifica e migrazione verso nuovi formati o supporti.

SPID: Sistema Pubblico di Identità Digitale

Identità digitale unica

SPID è un sistema di autenticazione che permette ai cittadini di accedere ai servizi online della Pubblica Amministrazione e dei privati aderenti con un'unica identità digitale. È utilizzabile da computer, tablet e smartphone e garantisce la piena protezione dei dati personali.

Processo di autenticazione

Il processo di login con SPID prevede che l'utente selezioni il proprio Identity Provider dalla lista disponibile sul sito del servizio, venga reindirizzato alla pagina di login dell'IdP, inserisca le proprie credenziali e, dopo la verifica, acceda al servizio richiesto.

Livelli di sicurezza

SPID prevede tre livelli di sicurezza crescenti, in base alla sensibilità dei servizi a cui si accede: livello 1 (username e password), livello 2 (+ password temporanea OTP), livello 3 (+ dispositivi fisici come smart card). Ogni servizio richiede il livello minimo necessario.

SPID: processo di ottenimento

Preparazione documenti

Documento d'identità valido, tessera sanitaria, email e numero di telefono cellulare

Scelta Identity Provider

Selezione di uno dei gestori accreditati in base a costi e modalità di riconoscimento

Riconoscimento

Identificazione personale via webcam, di persona, CIE, CNS o firma digitale

Attivazione

Ricezione delle credenziali e primo accesso al sistema

I requisiti fondamentali per ottenere SPID includono la maggiore età, un documento di identità italiano valido, la tessera sanitaria con codice fiscale, un indirizzo email personale e un numero di cellulare attivo. Per i cittadini italiani residenti all'estero, è necessario un documento d'identità italiano valido e un'iscrizione all'AIRE (Anagrafe degli Italiani Residenti all'Estero).

Gli Identity Provider accreditati sono organismi privati che, previa autorizzazione di AgID, forniscono le identità digitali SPID e gestiscono l'autenticazione degli utenti. Attualmente in Italia sono operativi nove Identity Provider: Aruba, Infocert, Intesa, Lepida, Namirial, Poste Italiane, Register, Sielte e TIM. Ogni provider offre modalità di riconoscimento e piani tariffari differenti, permettendo al cittadino di scegliere l'opzione più conveniente per le proprie esigenze.

SPID: vantaggi per cittadini e PA

Vantaggi per i cittadini

L'adozione di SPID porta numerosi benefici ai cittadini nella loro interazione con la Pubblica Amministrazione e i servizi privati aderenti:

- Accesso unificato a migliaia di servizi online con un'unica credenziale
- Eliminazione della necessità di ricordare diverse password per ogni servizio
- Riduzione dei tempi per le pratiche amministrative
- Possibilità di completare procedure da remoto senza recarsi agli sportelli
- Maggiore sicurezza rispetto a sistemi di autenticazione tradizionali
- Controllo sui propri dati personali e sulla loro condivisione

Vantaggi per la PA

Il Sistema Pubblico di Identità Digitale offre significativi vantaggi anche alle amministrazioni pubbliche:

- Semplificazione dei processi di registrazione e autenticazione degli utenti
- Riduzione dei costi per la gestione di sistemi proprietari di identità digitale
- Maggiore sicurezza e affidabilità nell'identificazione degli utenti
- Diminuzione degli errori nei processi amministrativi
- Standardizzazione delle procedure di accesso ai servizi
- Conformità automatica agli standard di sicurezza più recenti

CIE: Carta d'Identità Elettronica

Caratteristiche fisiche

La CIE è una smart card in policarbonato delle dimensioni di una carta di credito. È dotata di un microprocessore che memorizza in modo sicuro i dati personali, di un elemento olografico di sicurezza e di un QR code. Sul retro è presente la firma del titolare, il codice fiscale sotto forma di codice a barre e l'MRZ (Machine Readable Zone) per la lettura automatica ai varchi di controllo.

Funzionalità digitali

Oltre a essere un documento di riconoscimento fisico, la CIE è anche uno strumento di identità digitale che permette:

- Autenticazione online ai servizi della PA con massimo livello di sicurezza
- Firma elettronica avanzata per documenti digitali
- Verifica dell'identità tramite app CieID su smartphone con NFC
- Accesso sicuro a servizi fisici come trasporti pubblici o biblioteche

Differenze rispetto a SPID

A differenza di SPID, la CIE:

- È un documento di identità fisico oltre che digitale
- Viene rilasciata esclusivamente dal Ministero dell'Interno tramite i Comuni
- Ha una validità temporale legata alla scadenza del documento (10 anni)
- Richiede sempre l'identificazione di persona allo sportello comunale
- Offre nativamente il massimo livello di sicurezza (equivalente a SPID livello 3)

CIE: processo di rilascio

Prenotazione appuntamento

Il cittadino prenota un appuntamento presso l'ufficio anagrafe del proprio Comune di residenza, utilizzando i sistemi di prenotazione online o telefonici messi a disposizione dall'amministrazione locale. Alcuni Comuni offrono anche la possibilità di recarsi direttamente allo sportello senza prenotazione.

Presentazione allo sportello

All'appuntamento, il cittadino deve presentarsi con una fototessera recente in formato cartaceo o digitale, il codice fiscale o tessera sanitaria, il vecchio documento d'identità (se in possesso) e la ricevuta di pagamento del costo della CIE (attualmente 22,21 euro). In caso di primo rilascio o smarrimento, è necessaria la presenza di due testimoni o altro documento di riconoscimento.

Acquisizione dati

L'operatore comunale acquisisce i dati biometrici del cittadino (fotografia e impronte digitali) e verifica l'identità del richiedente. Le impronte digitali vengono memorizzate nel chip della carta ma non sono conservate in alcuna banca dati centrale, in conformità con le normative sulla privacy.

Consegna della carta

La CIE non viene rilasciata immediatamente, ma viene prodotta dall'Istituto Poligrafico e Zecca dello Stato e recapitata all'indirizzo indicato dal cittadino tramite posta raccomandata, generalmente entro 6 giorni lavorativi dalla richiesta. Al momento della consegna, viene fornito anche il PIN/PUK in due parti: la prima allo sportello comunale, la seconda nella lettera che accompagna la carta.

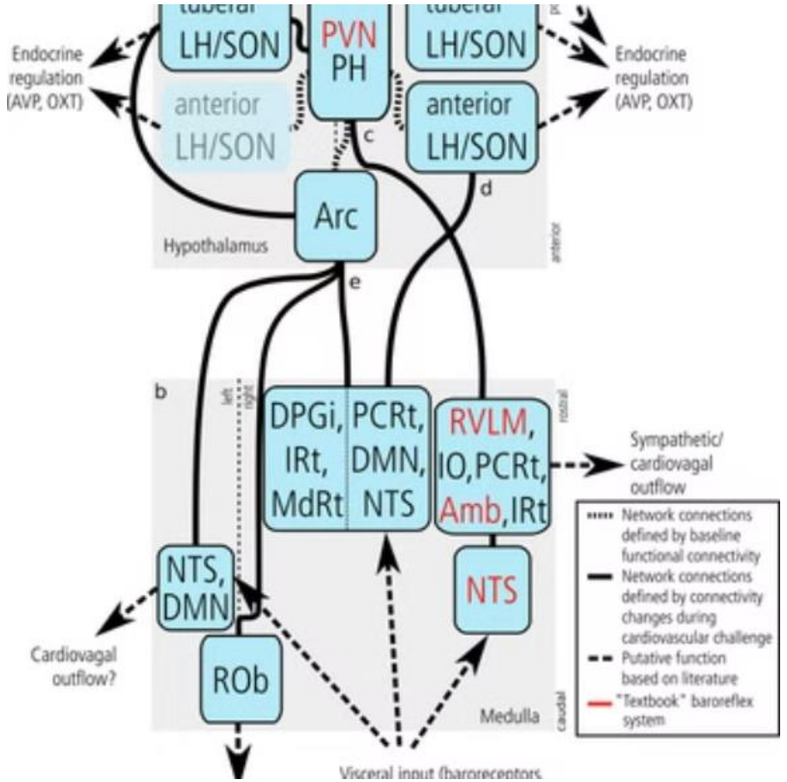
Altri sistemi di identità digitale

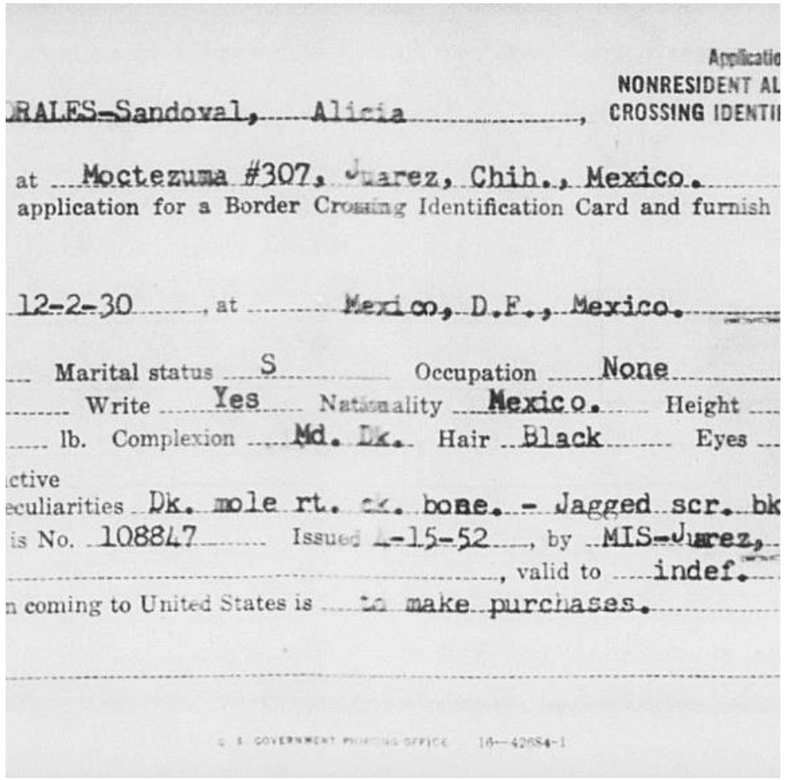
1998	15M	5
CNS - Prima introduzione	Tessere sanitarie attive	Sistemi regionali
Anno di introduzione della Carta Nazionale dei Servizi	Con funzionalità di CNS in Italia	Principali identità digitali regionali ancora attive

La **Carta Nazionale dei Servizi (CNS)** è una smart card che permette l'autenticazione in rete verso la Pubblica Amministrazione. Spesso è integrata nella Tessera Sanitaria (TS-CNS) e richiede un lettore di smart card per l'utilizzo. Anche se gradualmente sostituita da SPID e CIE, la CNS rimane ancora valida per l'accesso a molti servizi pubblici, soprattutto in ambito sanitario e nel rapporto con le amministrazioni locali.

Diverse regioni italiane hanno sviluppato **sistemi di identità digitale propri** prima dell'avvento di SPID, alcuni dei quali sono ancora attivi. Tra questi, FedERa in Emilia-Romagna, Sistema Piemonte in Piemonte, Carta Regionale dei Servizi in Lombardia, LepidaID in Emilia-Romagna e SPID Lombardia. Questi sistemi regionali stanno progressivamente convergendo verso lo SPID nazionale, ma mantengono alcune specificità per servizi locali.

eIDAS: identità digitale europea





RALES-Sandoval, Alicia

at Moctezuma #307, Juarez, Chih., Mexico.

application for a Border Crossing Identification Card and furnish

12-2-30, at Mexico, D.F., Mexico.

Marital status S Occupation None

Write Yes Nationality Mexico. Height

lb. Complexion Md. Dk. Hair Black Eyes

Peculiarities Dk. mole rt. ck. bone. - Jagged scr. bk

is No. 108847 Issued 4-15-52, by MIS-Juarez,

, valid to indef.

n coming to United States is to make purchases.

eIDAS (electronic IDentification, Authentication and trust Services) è il regolamento UE n. 910/2014 che stabilisce un quadro normativo comune per i sistemi di identità digitale, le firme elettroniche e i servizi fiduciari in tutta l'Unione Europea. L'obiettivo principale è garantire l'interoperabilità transfrontaliera dei servizi pubblici digitali, permettendo ai cittadini di un paese membro di utilizzare la propria identità digitale nazionale per accedere ai servizi pubblici online di altri stati membri.

Il regolamento definisce tre livelli di garanzia per i sistemi di identità digitale (basso, significativo, elevato) in base al grado di affidabilità nell'identificazione delle persone. SPID e CIE sono stati notificati dall'Italia alla Commissione Europea come schemi di identità digitale conformi a eIDAS: SPID ai livelli "basso" e "significativo", mentre la CIE al livello "elevato". Questa notifica rende obbligatorio per gli altri stati membri accettare queste identità digitali italiane per l'accesso ai propri servizi pubblici online.

Single Sign-On nella PA

Concetto di Single Sign-On

Il Single Sign-On (SSO) è una tecnologia che permette agli utenti di autenticarsi una sola volta e accedere a più applicazioni o servizi correlati senza dover ripetere l'operazione di login. Una volta effettuata l'autenticazione, l'identità dell'utente viene gestita da un sistema centrale che comunica con le diverse applicazioni, autorizzando l'accesso senza richiedere nuovamente le credenziali.

Vantaggi del SSO

L'implementazione del SSO nella Pubblica Amministrazione offre numerosi vantaggi: migliora significativamente l'esperienza utente eliminando la necessità di gestire e ricordare multiple credenziali; aumenta la sicurezza concentrando l'autenticazione in un unico punto fortemente protetto; riduce il carico di lavoro degli help desk per problemi legati alle password; semplifica la gestione delle autorizzazioni e degli accessi; facilita l'adozione di servizi digitali da parte dei cittadini.

Implementazione con SPID e CIE

In Italia, SPID e CIE fungono da sistemi di SSO federato per la Pubblica Amministrazione. L'integrazione avviene tramite protocolli standard come SAML 2.0 (per SPID) e OpenID Connect (per CIE). Le amministrazioni che vogliono implementare il SSO devono seguire le linee guida tecniche fornite da AgID, configurare i propri servizi come Service Provider e registrarsi formalmente nel circuito di federazione. Il cittadino può così navigare tra diversi servizi della PA senza dover ripetere il login.

Futuro dell'identità digitale in Italia

IT Wallet (2024-2025)

Implementazione del portafoglio digitale italiano come estensione dell'app IO, che permetterà di custodire in modo sicuro documenti digitali, certificati e credenziali. Includerà inizialmente patente di guida, tessera sanitaria e carta europea della disabilità.

Evoluzione SPID-CIE (2023-2027)

Progressiva convergenza tra SPID e CIE verso un unico sistema nazionale di identità digitale che combinerà i punti di forza di entrambi. Prevede maggiore interoperabilità, estensione ai minori e nuove funzionalità di delega digitale.

EUDI Wallet (2025-2026)

Integrazione con il wallet digitale europeo previsto dal regolamento eIDAS 2.0, che consentirà l'utilizzo dell'identità digitale in tutti i paesi UE. Potrà contenere anche qualifiche professionali, titoli di studio e dati sanitari essenziali.

Setup dell'ambiente di lavoro

Software richiesti

Per completare il laboratorio, è necessario installare i seguenti software sul proprio computer:

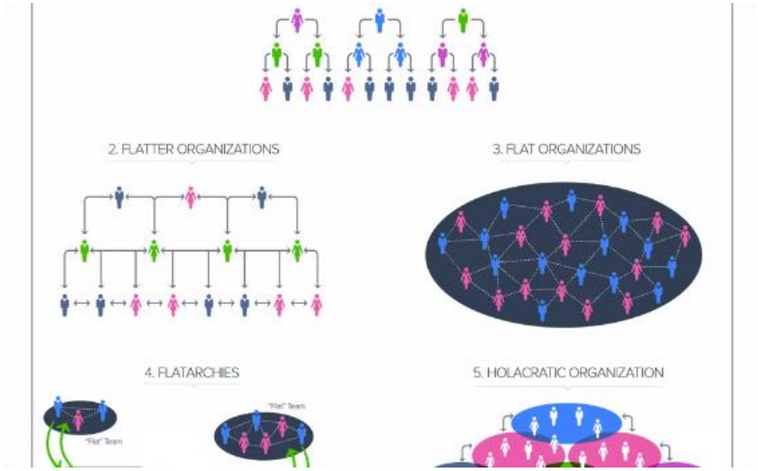
- Adobe Acrobat Reader DC (per visualizzazione e verifica PDF firmati)
- Dike o Aruba Sign (software di firma digitale)
- Driver per il proprio dispositivo di firma (smart card o token USB)
- Software di verifica firma AgID (Digital Signature Verifier)
- File Protector (per le firme CAdES)

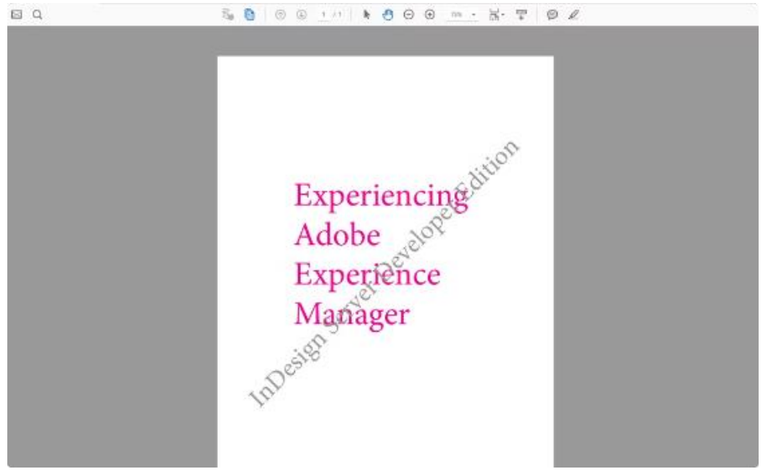
Configurazione iniziale

Una volta installati i software necessari, occorre procedere con la seguente configurazione:

- Collegare il lettore di smart card al computer e installare i driver
- Inserire il dispositivo di firma e verificarne il riconoscimento dal sistema
- Configurare il software di firma con i propri certificati
- Verificare la validità del certificato di firma
- Creare una cartella dedicata sul desktop per i file di esercitazione

Creazione di un documento PDF





Scelta del contenuto

Per il nostro esercizio pratico, creeremo un documento PDF che simula una determina dirigenziale della PA. Il documento dovrà contenere: intestazione dell'ente, numero di protocollo, data, oggetto, premesse normative, dispositivo (la decisione vera e propria) e la formula di sottoscrizione. Utilizzeremo un linguaggio formale tipico degli atti amministrativi e includeremo riferimenti normativi pertinenti.

Formattazione adeguata

La formattazione del documento è importante non solo per l'aspetto estetico ma anche per la corretta applicazione della firma digitale. È consigliabile utilizzare un layout chiaro con margini sufficienti, soprattutto nella parte inferiore dove verrà posizionata la firma visibile. Il documento dovrebbe essere strutturato in sezioni ben definite con titoli e sottotitoli, utilizzando un font leggibile come Arial o Times New Roman in dimensione 11-12pt.

Metadati e proprietà

Prima di salvare il documento, è importante compilare correttamente i metadati nelle proprietà del file: titolo, autore, oggetto e parole chiave. Questi metadati facilitano la ricerca e l'indicizzazione del documento nei sistemi di gestione documentale. Assicuratevi inoltre che il PDF sia conforme allo standard PDF/A per garantirne la conservazione a lungo termine e l'accessibilità.

Applicazione della firma digitale

Selezione del certificato

Dopo aver aperto il software di firma digitale, il primo passo consiste nel selezionare il certificato da utilizzare. Se disponete di più certificati (ad esempio personale e professionale), scegliete quello appropriato per il contesto. Verificate che il certificato non sia scaduto e che contenga correttamente i vostri dati identificativi.

Scelta del tipo di firma

Decidete quale formato di firma utilizzare: PAdES per mantenere il documento in formato PDF accessibile con qualsiasi lettore, o CAdES se desiderate una firma che possa essere applicata a qualsiasi tipo di file (risulterà in un file con estensione .p7m). Per questo esercizio, utilizzeremo entrambi i formati per confrontarne le caratteristiche.

Configurazione della firma visibile

Nel caso di firma PAdES, potete scegliere di rendere la firma visibile nel documento inserendo un'immagine grafica. Configurate l'aspetto della firma selezionando un'immagine (ad esempio un facsimile della vostra firma autografa), dimensione, posizione e informazioni da visualizzare (nome, data, motivo della firma).

Inserimento del PIN e conferma

Inserite il PIN associato al vostro dispositivo di firma per autorizzare l'operazione. Il software procederà con il calcolo dell'hash del documento, la cifratura con la vostra chiave privata e l'incorporazione della firma nel documento. Al termine, verrà generato il file firmato che potrete salvare con un nome che ne indichi lo stato (ad esempio "documento_firmato.pdf").

Verifica della firma digitale

Utilizzo di strumenti online

Per verificare l'autenticità e la validità di una firma digitale, esistono diversi strumenti disponibili. Utilizzeremo sia il verificatore ufficiale di AgID che strumenti alternativi per confrontare i risultati:

1. Accedere al sito web del verificatore AgID (Digital Signature Verification)
2. Caricare il documento firmato attraverso l'apposita interfaccia
3. Attendere l'elaborazione e l'analisi della firma
4. Ripetere la verifica con Adobe Acrobat Reader (per firme PAdES)
5. Confrontare i risultati ottenuti dai diversi strumenti

In alternativa, è possibile utilizzare software desktop come VerificaC o i programmi di verifica forniti dai certificatori accreditati.

Interpretazione dei risultati

L'esito della verifica può contenere diverse informazioni che è importante saper interpretare:

- **Firma valida**: indica che la firma è stata creata con un certificato valido e il documento non è stato alterato
- **Firmatario**: mostra i dati identificativi di chi ha apposto la firma
- **Certificato qualificato**: conferma che la firma è stata apposta con un certificato che rispetta i requisiti di legge
- **Periodo di validità**: indica se il certificato era valido al momento della firma
- **Riferimento temporale**: mostra data e ora della firma
- **Revoca/sospensione**: verifica che il certificato non fosse revocato al momento della firma
- **Integrità**: conferma che il documento non ha subito modifiche dopo la firma

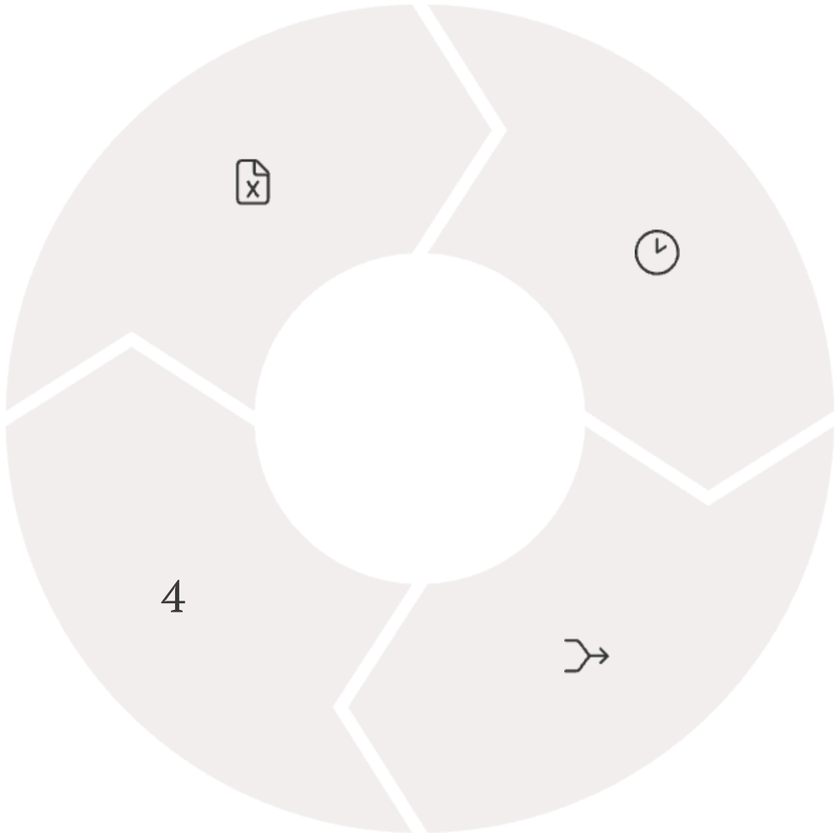
Applicazione della marca temporale

Preparazione del documento

Verificare che il documento sia già firmato digitalmente

Richiesta marca temporale

Utilizzare il servizio di timestamping del certificatore



Verifica del risultato

Controllare la validità della marca e della firma

Integrazione con la firma

Associare la marca temporale al documento firmato

La marca temporale è uno strumento essenziale per garantire la validità legale di un documento firmato digitalmente anche dopo la scadenza del certificato di firma. In questo esercizio pratico, applicheremo una marca temporale a un documento già firmato, utilizzando il servizio di timestamping fornito dal nostro certificatore qualificato.

Esploreremo le due principali modalità di applicazione della marca temporale: inserita direttamente nel documento firmato (per firme PAdES) o come file separato con estensione .tsr o .tst (per firme CAdES). In entrambi i casi, verificheremo che la marca sia stata correttamente apposta controllando che la data e l'ora siano accurate e che la marca provenga effettivamente da una Time Stamping Authority accreditata. Discuteremo inoltre le situazioni in cui l'apposizione della marca temporale è obbligatoria secondo la normativa italiana.

Firma remota

La **firma remota** (o firma digitale remota) è una soluzione tecnologica che consente di firmare documenti elettronici attraverso un servizio online, senza necessità di dispositivi fisici come smart card o token USB. Il certificato di firma viene conservato presso un server sicuro del certificatore accreditato, accessibile solo tramite credenziali personali e sistemi di autenticazione forte.

I principali vantaggi della firma remota includono:

Accessibilità

Possibilità di firmare da qualsiasi dispositivo connesso a internet

Sicurezza avanzata

Utilizzo di sistemi di autenticazione a più fattori per proteggere il certificato

Semplicità gestionale

Nessuna necessità di aggiornare o sostituire dispositivi fisici

La firma remota sta guadagnando popolarità nella Pubblica Amministrazione grazie alla sua flessibilità e facilità d'uso. Il processo di firma tipicamente richiede un'autenticazione a due fattori per garantire la massima sicurezza: dopo l'accesso con username e password, l'utente riceve un codice OTP (One-Time Password) sul proprio dispositivo mobile per autorizzare l'operazione.

Le soluzioni di firma remota devono comunque rispettare tutti i requisiti di sicurezza e validità legale previsti dalla normativa italiana ed europea, garantendo lo stesso valore giuridico delle firme apposte con dispositivi fisici.

Verifica di firme PAdES, XAdES, CAdES

Formato	Strumento di verifica	Elementi da controllare
PAdES	Adobe Acrobat Reader / DSV AgID	Pannello firme, validità, visualizzazione
XAdES	Verificatore XAdES / DSV AgID	Schema XML, integrità, certificati
CAdES	File Protector / DSV AgID	Estrazione contenuto, catena di certificazione

In questa parte del laboratorio, esamineremo le differenze nel processo di verifica per i tre principali formati di firma digitale utilizzati nella Pubblica Amministrazione. Utilizzeremo documenti preconfezionati firmati nei diversi formati e analizzeremo le specificità di ciascun processo di verifica.

Per le firme PAdES, ci concentreremo sull'interpretazione del pannello firme di Adobe Acrobat Reader e sul controllo delle proprietà di firma visibili. Per le firme XAdES, utilizzeremo strumenti specializzati che permettono di navigare nella struttura XML e verificare gli elementi di firma incorporati. Per le firme CAdES, praticheremo l'estrazione del contenuto originale dal file .p7m e la verifica della catena di certificazione. In tutti i casi, evidenzieremo le potenziali criticità e gli errori più comuni che possono emergere durante la verifica, come problemi con i certificati revocati, timestamp non validi o documenti alterati dopo la firma.

Gestione degli errori comuni

Problemi di riconoscimento del dispositivo

Uno degli errori più frequenti riguarda il mancato riconoscimento del dispositivo di firma (smart card o token USB) da parte del sistema operativo o del software di firma. Le soluzioni tipiche includono:

- Reinstallazione dei driver più recenti del dispositivo
- Utilizzo di una porta USB differente (preferibilmente USB 2.0 per i token)
- Verifica della compatibilità con il sistema operativo
- Riavvio del computer dopo l'installazione dei driver

Errori di PIN

I problemi relativi al PIN rappresentano un'altra categoria comune di errori:

- Blocco del dispositivo dopo ripetuti tentativi errati
- Dimenticanza del PIN
- Malfunzionamento della tastiera virtuale per l'inserimento

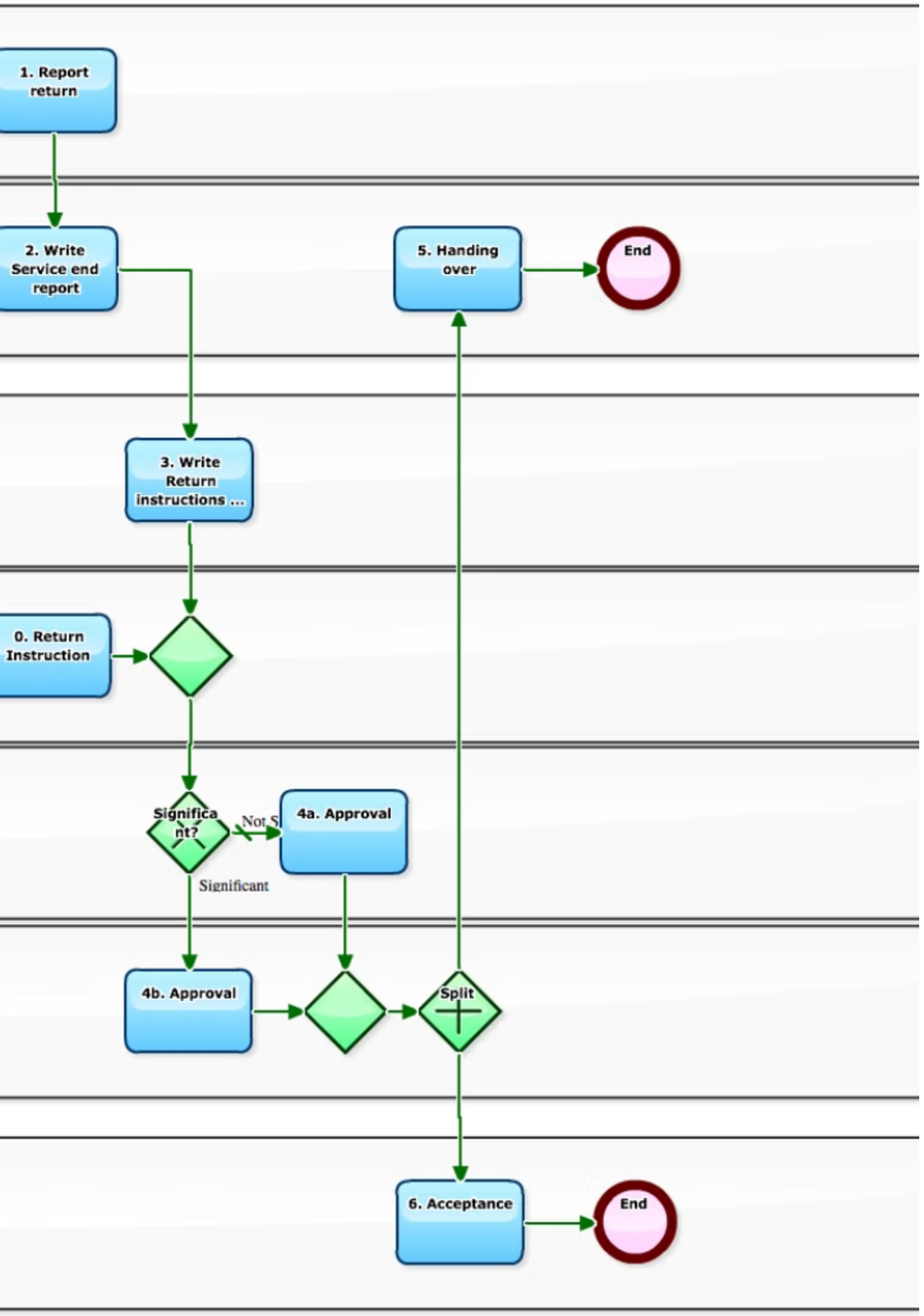
È importante sapere che dopo un certo numero di tentativi falliti (generalmente 3), il dispositivo si blocca e può essere sbloccato solo con il PUK. Se anche il PUK viene bloccato, il dispositivo diventa inutilizzabile e va sostituito.

Problemi con i certificati

Altri errori comuni riguardano i certificati digitali:

- Certificato scaduto o prossimo alla scadenza
- Certificato revocato (ad esempio per smarrimento del dispositivo)
- Impossibilità di verificare lo stato del certificato (problemi di connessione ai server OCSP o CRL)
- Certificato non qualificato utilizzato per operazioni che richiedono una firma qualificata

È fondamentale monitorare la scadenza dei propri certificati e procedere al rinnovo con adeguato anticipo.



Conservazione dei documenti firmati

1

Verifica preliminare

- Controllo dell'integrità del documento
- Verifica della validità di tutte le firme
- Controllo della presenza di marche temporali
- Verifica del formato (preferibilmente PDF/A per la conservazione)

Metadatazione

- Creazione dell'indice di classificazione
- Associazione dei metadati rilevanti (tipologia, autore, data, oggetto, etc.)
- Collegamento con il fascicolo di appartenenza
- Generazione di identificativi univoci

Invio al sistema di conservazione

- Trasmissione sicura al conservatore accreditato
- Verifica della corretta ricezione
- Acquisizione della ricevuta di versamento
- Registrazione degli estremi di conservazione

Verifica della reperibilità

- Test di ricerca del documento nel sistema
- Controllo dell'accessibilità e visualizzazione
- Verifica del mantenimento dell'integrità
- Simulazione di procedura di esibizione a norma

Integrazione con SPID: caso pratico

Ambiente di test

In questo esercizio utilizzeremo l'ambiente di test ufficiale di SPID, che permette di simulare l'intero processo di autenticazione senza utilizzare credenziali reali. Questo ambiente è disponibile per sviluppatori e amministratori IT per testare l'integrazione di SPID nei propri servizi prima di passare all'ambiente di produzione.

Configurazione del servizio

Esploreremo i passaggi necessari per configurare un servizio di test che accetta l'autenticazione SPID. Questo include la registrazione come Service Provider, la generazione delle chiavi crittografiche, la configurazione dei metadata SAML e l'implementazione del flusso di autenticazione secondo le specifiche tecniche AgID.

Simulazione dell'accesso

Dimostreremo l'intero flusso di autenticazione SPID dal punto di vista dell'utente, utilizzando le identità di test fornite dall'ambiente di demo. Analizzeremo le schermate di redirect, la selezione dell'Identity Provider, l'inserimento delle credenziali e il ritorno al servizio con l'identità verificata.

Analisi della sicurezza

Esamineremo gli aspetti di sicurezza dell'integrazione SPID, come la protezione dei messaggi SAML, la validazione delle firme, la gestione delle sessioni e la protezione contro attacchi comuni come il replay attack o il man-in-the-middle.

Utilizzo della CIE per l'autenticazione

Setup dell'hardware

Per utilizzare la CIE come strumento di autenticazione ai servizi digitali, è necessario dotarsi di un lettore di smart card compatibile con le specifiche della carta. In questo esercizio, utilizzeremo un lettore a contatto standard conforme agli standard PC/SC e installeremo i driver necessari. In alternativa, per chi dispone di uno smartphone con tecnologia NFC, mostreremo l'utilizzo dell'app CieID per l'autenticazione senza lettore fisico.

Installazione del middleware CIE

Il passo successivo consiste nell'installazione del software CIE (Middleware) sul computer. Questo software, disponibile sul sito del Ministero dell'Interno, funge da intermediario tra la carta, il lettore e le applicazioni che richiedono l'autenticazione. Il middleware è disponibile per Windows, macOS e Linux, e il suo funzionamento corrisponde agli standard internazionali per le carte d'identità elettroniche.

Configurazione del browser

Per utilizzare la CIE con i servizi online, è necessario configurare correttamente il browser. In particolare, verificheremo che il middleware CIE sia riconosciuto come provider di certificati dal browser e che le impostazioni di sicurezza permettano l'interazione con il lettore di smart card. Mostreremo la configurazione su diversi browser (Chrome, Firefox, Edge) evidenziando le differenze.

Processo di login con CIE

Infine, simuleremo un accesso a un servizio pubblico utilizzando la CIE come metodo di autenticazione. Seguiremo il flusso completo: selezione del pulsante "Entra con CIE" sul sito del servizio, inserimento della carta nel lettore, digitazione del PIN e reindirizzamento al servizio con identità verificata. Analizzeremo anche gli eventuali problemi comuni e le relative soluzioni.

Esercizio finale: workflow completo

1 Creazione

Redazione di una determina dirigenziale in formato PDF/A con metadati completi e struttura conforme alle normative

2 Firma

Apposizione di firma digitale PAdES con marca temporale e configurazione della rappresentazione visibile

3 Verifica

Controllo dell'autenticità e validità della firma utilizzando strumenti ufficiali e analisi dei risultati

4 Conservazione

Preparazione per l'invio in conservazione con metadatazione completa e verifica dell'integrità

In questo esercizio finale, metteremo in pratica tutte le competenze acquisite durante il laboratorio, simulando un workflow documentale completo tipico della Pubblica Amministrazione. Partiremo dalla creazione di un documento amministrativo autentico (una determina dirigenziale) che includa tutti gli elementi formali richiesti dalla normativa, compresa la corretta intestazione e struttura.

Procederemo poi con l'apposizione di una firma digitale qualificata, configurando attentamente sia gli aspetti tecnici (formato, algoritmi, inclusione della marca temporale) sia quelli visuali (posizionamento della firma visibile, informazioni da mostrare). Verificheremo quindi l'autenticità del documento firmato utilizzando diversi strumenti e interpretando in dettaglio i risultati. Infine, prepareremo il documento per la conservazione a norma, creando il pacchetto di versamento con tutti i metadati necessari e simulando il processo di invio al sistema di conservazione.

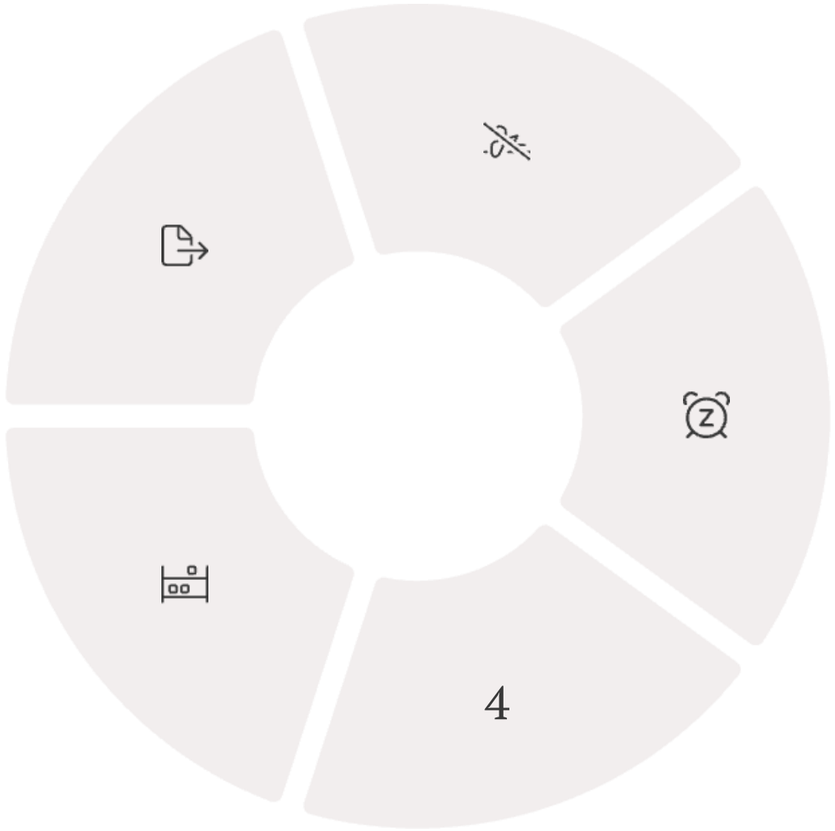
Recap e best practices

Formati aperti

Privilegiare sempre formati standardizzati e aperti (PDF/A, XML, CSV) per garantire l'interoperabilità e la conservazione a lungo termine. Evitare formati proprietari o binari per documenti ufficiali.

Conservazione

Progettare i processi documentali considerando fin dall'inizio i requisiti di conservazione a norma. Verificare periodicamente l'integrità e la leggibilità dei documenti conservati.



Firme digitali

Utilizzare il formato di firma più appropriato in base al contesto: PAdES per documenti che devono essere facilmente visualizzabili, XAdES per documenti strutturati che richiedono elaborazione automatica, CAdES per la massima versatilità.

Marche temporali

Applicare sempre una marca temporale ai documenti con rilevanza legale per garantirne la validità nel tempo, soprattutto se il documento dovrà essere conservato oltre la scadenza del certificato di firma.

Identità digitale

Implementare meccanismi di autenticazione basati su SPID e CIE per tutti i servizi rivolti ai cittadini. Garantire che il livello di sicurezza richiesto sia proporzionato alla sensibilità del servizio.

Il Protocollo Informatico nella Scuola

Il protocollo informatico rappresenta oggi uno strumento fondamentale per la digitalizzazione e l'efficienza delle istituzioni scolastiche italiane. Attraverso questo sistema, le scuole possono gestire in modo organizzato e sicuro tutta la documentazione amministrativa, garantendo trasparenza e conformità normativa.

Questa presentazione illustrerà i principi, le componenti e i vantaggi del protocollo informatico nel contesto scolastico, evidenziando come la sua corretta implementazione possa trasformare radicalmente i processi amministrativi delle scuole italiane.

Cos'è il Protocollo Informatico?

Definizione

Il protocollo informatico è un sistema di gestione documentale che consente la registrazione, classificazione e archiviazione di documenti in formato digitale. Rappresenta lo strumento attraverso cui le scuole garantiscono la tracciabilità dei documenti amministrativi.

Questo sistema permette di assegnare ad ogni documento un identificativo univoco (numero di protocollo) associato a data e ora di ricezione o produzione, garantendo così l'autenticità e l'integrità dei documenti nel tempo.

Normativa di riferimento

Il sistema si basa sul DPR 445/2000 (Testo Unico sulla Documentazione Amministrativa), sul Codice dell'Amministrazione Digitale (D.Lgs. 82/2005) e sulle linee guida AgID, che definiscono gli standard di gestione documentale per tutte le pubbliche amministrazioni.

Ulteriori disposizioni sono contenute nel DPCM 3 dicembre 2013 sulle regole tecniche per il protocollo informatico e nel DPCM 13 novembre 2014 riguardante la formazione e conservazione dei documenti informatici. Le circolari ministeriali specifiche per le istituzioni scolastiche completano il quadro normativo.

Evoluzione storica

L'introduzione del protocollo informatico nelle scuole italiane ha seguito un percorso graduale, iniziato nei primi anni 2000 con le prime sperimentazioni pilota. Dal 2016, con il Piano Nazionale Scuola Digitale (PNSD), ha subito un'accelerazione significativa.

Prima dell'adozione dei sistemi informatici, la protocollazione avveniva mediante registri cartacei, con evidenti limitazioni in termini di accessibilità, ricerca e conservazione. La transizione digitale ha rappresentato una rivoluzione nei processi amministrativi scolastici.

L'adozione del protocollo informatico non è solo un obbligo normativo, ma rappresenta un passaggio cruciale nel processo di modernizzazione della scuola italiana, permettendo l'abbandono graduale della documentazione cartacea in favore di processi completamente digitali e interoperabili.

Il sistema si integra con altri strumenti digitali della scuola come il registro elettronico e i sistemi di conservazione a norma, creando un ecosistema digitale coerente. Grazie a questa integrazione, il protocollo informatico diventa il fulcro della gestione documentale dell'istituzione scolastica, garantendo efficienza amministrativa, trasparenza e rispetto delle normative sulla privacy e sulla conservazione dei dati.

Obiettivi del Protocollo Informatico

Efficienza interna

Automazione dei processi amministrativi con conseguente riduzione dei tempi di gestione documentale e ottimizzazione delle risorse umane disponibili.

Razionalizzazione dei flussi

Organizzazione logica dei documenti che permette di seguire l'intero ciclo di vita della documentazione, dalla creazione all'archiviazione.

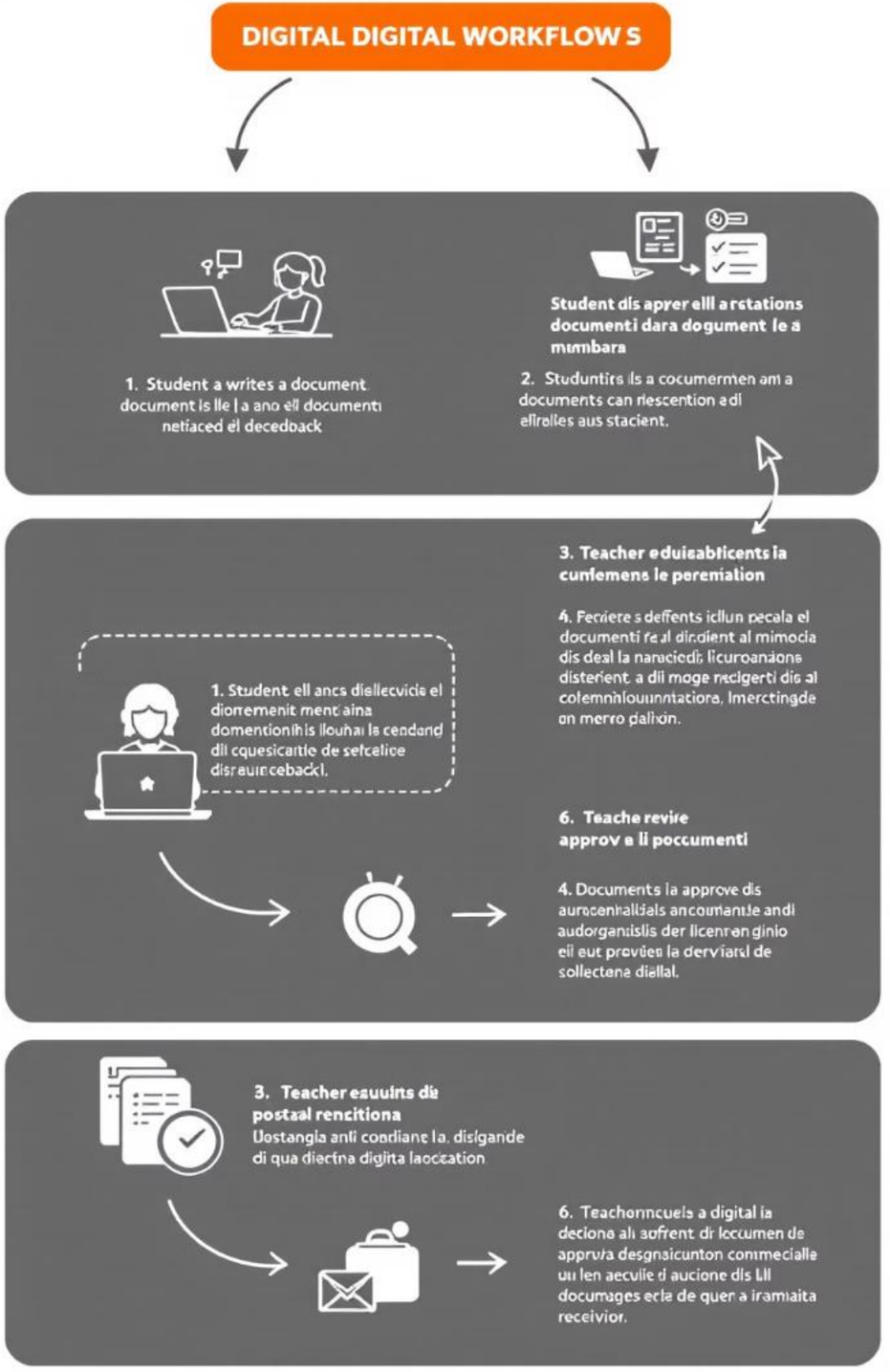
Trasparenza amministrativa

Garanzia di accesso alle informazioni e tracciabilità completa delle operazioni svolte sui documenti, in conformità ai principi di buona amministrazione.

Conservazione documentale

Archiviazione a norma dei documenti digitali che ne garantisce l'integrità, l'autenticità e la leggibilità nel tempo, rispettando i requisiti legali per la conservazione a lungo termine.

Il protocollo informatico mira a creare un sistema di gestione documentale integrato che elimini le inefficienze del sistema cartaceo tradizionale, garantendo al contempo la validità legale dei documenti digitali attraverso i meccanismi di autenticazione e firma digitale.



Componenti Chiave del Sistema

- **Workflow documentale:** Gestione completa del flusso di lavoro, dall'acquisizione alla distribuzione dei documenti, con monitoraggio in tempo reale dello stato di avanzamento delle pratiche
- **Gestione documentale:** Archiviazione strutturata e ricerca avanzata tramite metadati, con possibilità di recupero rapido dei documenti attraverso criteri multipli
- **Nucleo minimo di protocollo:** Registrazione cronologica e segnatura univoca dei documenti in entrata e in uscita, garantendo valore legale alle operazioni con numerazione cronologica azzerata ogni anno es: 10/2024, 1455/24, 8/25
- **Sistema di classificazione:** Titolario e piano di fascicolazione per l'organizzazione logica dei documenti secondo lo schema dell'amministrazione scolastica
- **Interoperabilità:** Capacità di comunicare con altri sistemi informatici della pubblica amministrazione attraverso standard condivisi
- **Sicurezza e accesso:** Sistemi di autenticazione e autorizzazione che garantiscono l'accesso controllato alle funzionalità in base ai ruoli assegnati

Il sistema di protocollo informatico si articola in diversi livelli di complessità, progettati per adattarsi alle specifiche esigenze dell'istituzione scolastica. Alla base troviamo il nucleo minimo che garantisce la registrazione cronologica dei documenti e la loro segnatura, elementi indispensabili per assicurare il valore legale delle comunicazioni. I livelli superiori aggiungono funzionalità avanzate come la fascicolazione elettronica, l'automazione dei processi amministrativi e l'integrazione con altri sistemi informativi.

Ruoli e Responsabilità

Dirigente Scolastico

Responsabile della corretta implementazione del sistema e della definizione delle politiche di sicurezza e accesso.

DSGA

Supervisiona la gestione operativa del protocollo informatico e coordina il personale amministrativo.

Referente PEC/PEO

Gestisce la posta elettronica certificata e ordinaria, integrandola con il sistema di protocollo.

Assistenti Amministrativi

Operatori del sistema che effettuano le registrazioni quotidiane e gestiscono la documentazione.

La chiara definizione dei ruoli è essenziale per il corretto funzionamento del protocollo informatico. Ogni figura professionale contribuisce con competenze specifiche: il Dirigente stabilisce le linee strategiche, il DSGA garantisce l'operatività quotidiana, mentre gli assistenti amministrativi rappresentano gli utenti principali del sistema.

Processo di Protocollazione

Ricezione documento

Acquisizione tramite canali fisici o digitali

Registrazione

Assegnazione numero progressivo

Classificazione

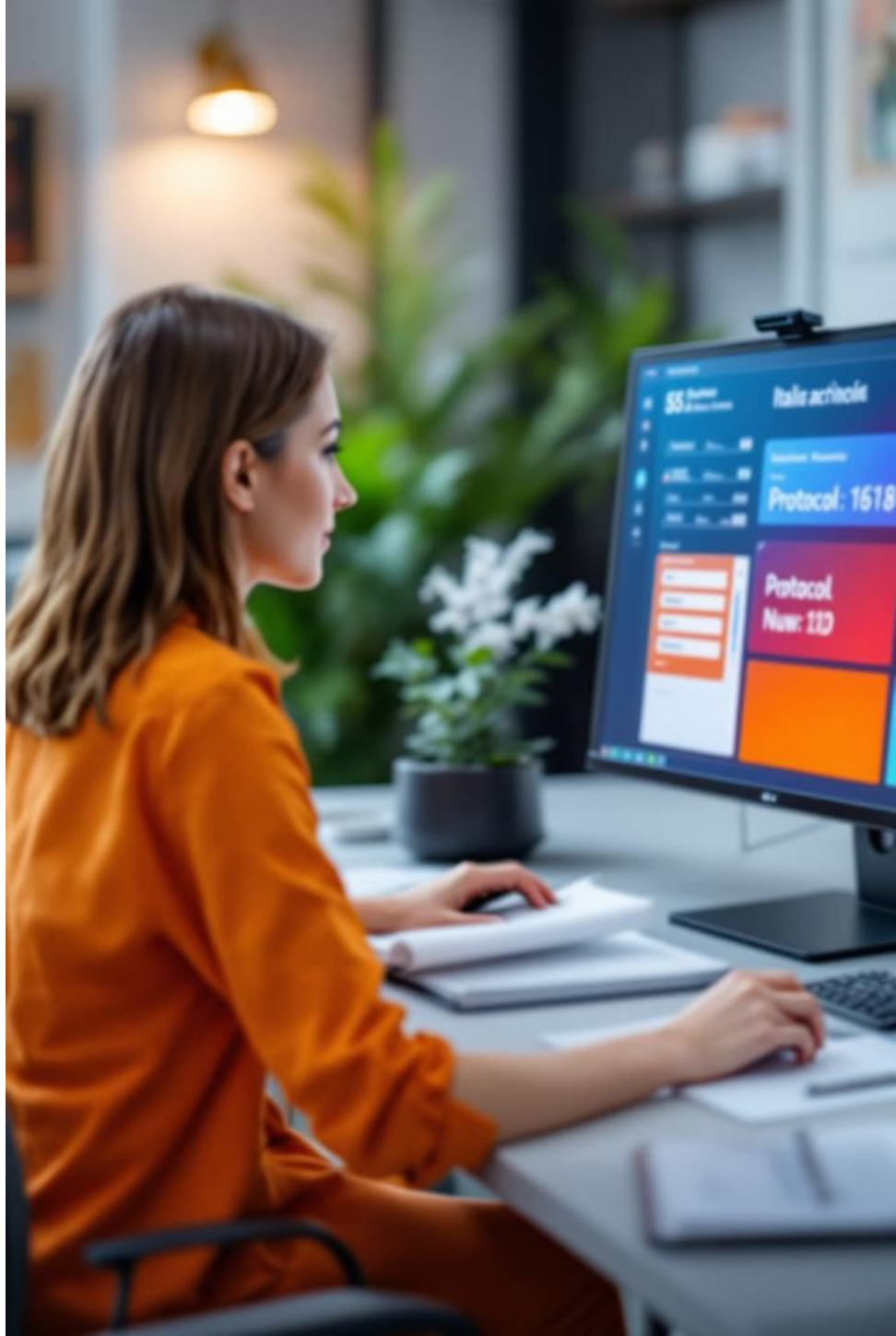
Categorizzazione per tipologia

Fascicolazione

Inserimento nel fascicolo appropriato

Il processo di protocollazione segue un flusso ben definito che garantisce l'univocità e la certezza temporale della registrazione. Ogni documento in entrata o in uscita riceve un numero di protocollo unico, accompagnato da data e ora di registrazione, classificazione tematica e assegnazione all'ufficio competente.

La segnatura di protocollo rappresenta l'impronta digitale del documento e contiene tutte le informazioni necessarie per identificarlo all'interno del sistema. Nei documenti digitali, la segnatura viene incorporata direttamente nel file tramite metadati strutturati.



Gestione dei Documenti Digitali

Formati e standard

I documenti digitali devono rispettare formati standard come PDF/A per garantire la leggibilità nel tempo. Le specifiche tecniche sono definite dalle linee guida AgID e includono requisiti di interoperabilità e accessibilità.

Firma digitale

Elemento essenziale per la validità legale dei documenti, la firma digitale garantisce autenticità, integrità e non ripudio. Il Dirigente Scolastico e il DSGA sono generalmente i titolari di firma nelle istituzioni scolastiche.

Conservazione a norma

Processo che garantisce il mantenimento del valore legale dei documenti nel tempo. Include la marcatura temporale e procedure specifiche di backup e verifica dell'integrità dei dati secondo la normativa vigente.

La gestione documentale digitale richiede particolare attenzione alla qualità e all'integrità dei documenti. L'adozione di standard aperti e l'utilizzo di sistemi di firma digitale qualificata sono requisiti fondamentali per garantire il valore legale della documentazione amministrativa scolastica nel lungo periodo.

Vantaggi per la Scuola

70%

Riduzione costi

Risparmio su carta, stampa e spazi fisici di archiviazione

85%

Efficienza

Miglioramento nell'accesso e gestione delle informazioni

60%

Comunicazione

Incremento nella qualità degli scambi informativi

L'adozione del protocollo informatico porta benefici tangibili all'istituzione scolastica. La riduzione dei costi operativi si manifesta non solo nel risparmio di materiali di consumo, ma anche nell'ottimizzazione delle risorse umane, che possono dedicare più tempo ad attività a valore aggiunto anziché alla ricerca e gestione di documentazione cartacea.

La rapidità di accesso alle informazioni migliora significativamente la qualità del servizio offerto all'utenza, permettendo risposte immediate alle richieste e una gestione più efficace della comunicazione sia interna che con l'esterno.

Sfide e Soluzioni

Formazione del personale

Pianificazione di corsi specifici per livelli di competenza digitale differenziati. Affiancamento continuo nelle fasi iniziali di implementazione e supporto tecnico dedicato per risolvere problematiche operative.

Sicurezza e privacy

Implementazione di sistemi di autenticazione forte con profili di accesso differenziati. Adozione di protocolli di sicurezza avanzati e configurazione del sistema in conformità al GDPR per la protezione dei dati personali.

Integrazione con sistemi esistenti

Sviluppo di connettori e API per garantire l'interoperabilità con software gestionali già in uso. Migrazione graduale dei dati dai sistemi legacy e periodo di coesistenza per evitare interruzioni nei servizi.

L'implementazione del protocollo informatico comporta sfide significative, particolarmente in contesti con limitata familiarità tecnologica. La resistenza al cambiamento rappresenta spesso l'ostacolo principale, superabile attraverso percorsi formativi strutturati e una comunicazione efficace sui benefici attesi.

Conclusioni e Prospettive Future

Digitalizzazione base

Implementazione del nucleo minimo di protocollo con registrazione e archiviazione digitale dei documenti essenziali.

1

Integrazione avanzata

Collegamento con altri sistemi gestionali della scuola e implementazione completa del workflow documentale.

2

Trasformazione digitale

Riprogettazione dei processi amministrativi in ottica completamente digitale con eliminazione del cartaceo.

3

Futuri sviluppi

Adozione di tecnologie emergenti come blockchain per la certificazione documentale e intelligenza artificiale per la classificazione automatica.

4

Il protocollo informatico rappresenta solo l'inizio del percorso di trasformazione digitale della scuola italiana. L'evoluzione naturale porterà a sistemi sempre più integrati e intelligenti, capaci di automatizzare processi complessi e fornire supporto decisionale avanzato.