Produzione, gestione e conservazione del documento digitale

Luciana Duranti
UNIDOC
Roma 30 giugno 2010

Digital Records Forensics Project

La Tradizione

Sir Hilary Jenkinson, *Manual of Archival Administration.* London, 1922.

- La prima responsabilità dell'archivista e proteggere i documenti
- La seconda responsabilità dell'archivista è guidare gli utenti

Proteggere i documenti

Significa mantenere intatte le loro caratteristiche:

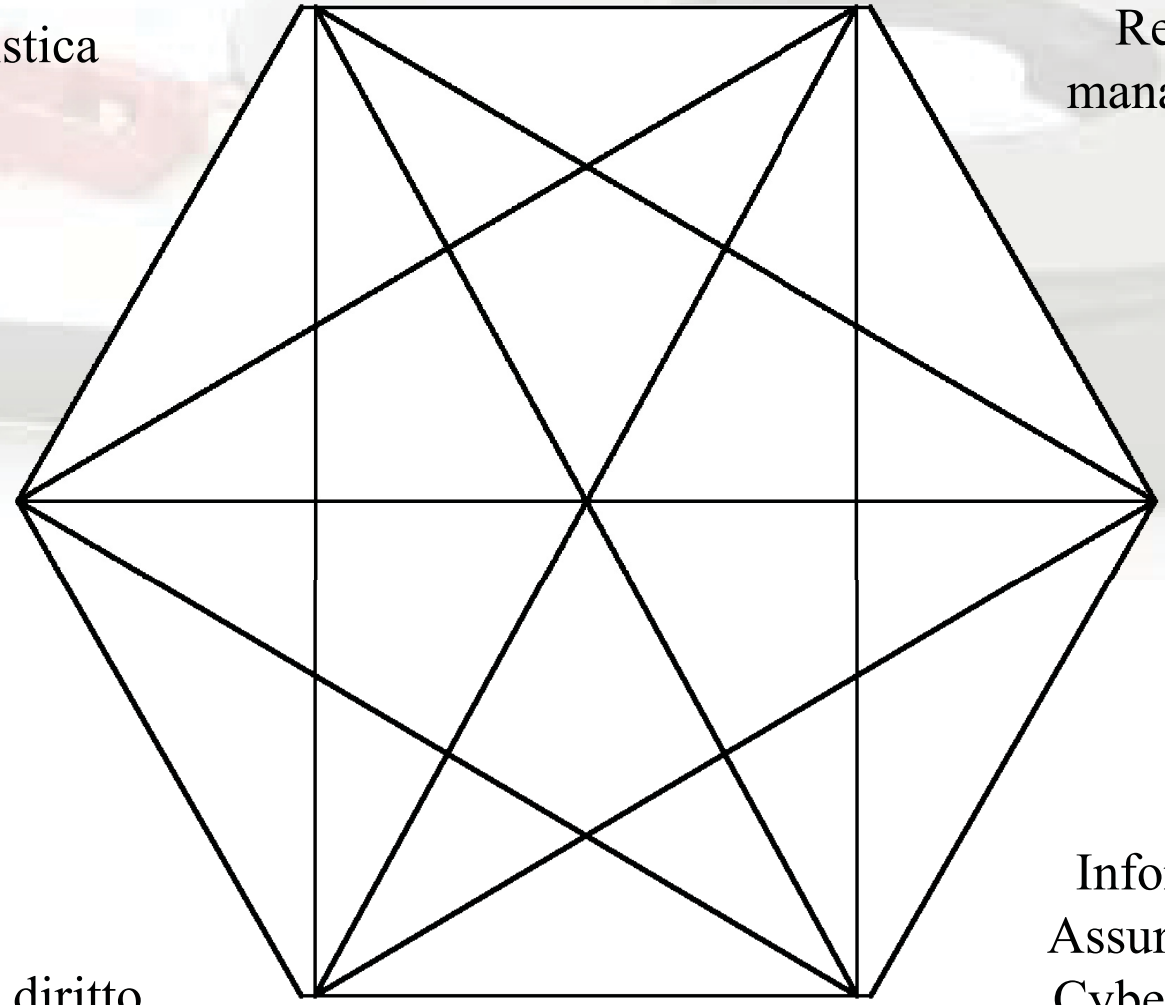
1. Naturalezza (naturalness)
2. Vincolo archivistico (interrelatedness)
3. Imparzialità (impartiality)
4. Autenticità (authenticity)

Metodo: una catena ininterrotta di legittima custodia (unbroken legitimate custody)

La natura della sfida

- Sistemi documentari ibridi
- Ambiente digitale che supporta manipolazione e repourposing dei dati
- Indifferenza del produttore dei documenti al problema della loro autenticità, dovuta a fiducia nella tecnologia
- Natura proprietaria e idiosincratica delle applicazioni
- Obsolescenza di supporti e di sistemi
- Assenza di un originale
- Caratteristiche del documento digitale

Quadro concettuale per l'analisi



Quadro concettuale per l'analisi

Diplomatica Digitale: lo sviluppo e l'applicazione della diplomatica classica ai documenti digitali

Digital Forensics: l'uso di metodi scientifici per l'acquisizione, la validazione, l'identificazione, l'analisi, l'interpretazione, la documentazione e la presentazione di fonti digitali di prova allo scopo di facilitare la ricostruzione di eventi criminali o anticipare atti non autorizzati che possono danneggiare operazioni pianificate

In particolare, abbiamo bisogno di conoscenze interdisciplinari che, una volta integrate, potrebbero essere definite **"Digital Records Forensics"**.

Quadro concettuale per l'analisi

Contributi della diplomatica

- Concetto di documento digitale
- Concetti di affidabilità, accuratezza, autenticità e autenticazione

Contributi di digital forensics:

- Processo affidabile di estrazione o reproduzione
- Categorizzazione dei documenti digitali
- Distinzione tra integrità di documenti e di riproduzioni
- Regole per la determinazione dell'integrità di sistemi
- Principi di non-interferenza e interferenza identificabile
- Principi per determinare autenticità
- Basi per l'autenticazione

Il concetto di documento

Un documento archivistico è un documento prodotto, cioè generato o ricevuto e archiviato, da una persona fisica o giuridica nel corso di un'attività pratica come suo strumento e residuo
documento è informazione affissa ad un supporto in una forma determinata
informazione è un messaggio comunicato attraverso lo spazio o il tempo e composto di dati
dato è il più piccolo pezzo di informazione che abbia significato

Un documento digitale è un documento il cui contenuto e la cui forma sono codificati usando valori numerici distinti (come i valori binari 0 e 1) piuttosto che uno spettro continuo di valori (come quelli generati da un sistema analogico).

Un documento elettronico è un documento analogico o digitale che viene trasportato da un conduttore elettrico e richiede l'uso di tecnologie per essere reso intellegibile a una persona

Caratteristiche di un documento digitale

- Vincolo esplicito con gli altri documenti interni o esterni al sistema digitale per mezzo di un codice di classificazione o di un altro identificatore unico
- Un contesto amministrativo identificabile
- Un autore, un destinatario, uno scrittore, un produttore, un originatore
- Un atto in cui il documento partecipa o a cui il documento fornisce supporto o proceduralmente o come parte di un processo decisionale
- Contenuto stabile
- Forma fissa

Contenuto stabile

- I dati e il messaggio nel documento sono immutati dal momento in cui sono stati scritti, e inalterabili
- Non è possibile scrivere sopra dati esistenti, alterarli, o cancellarli
- Non è possibile aggiungere dati alla prima manifestazione del documento

Forma fissa

- Il contenuto binario è affisso al supporto in modo da rimanere completo e inalterato e il messaggio può essere reso con la stessa forma documentaria che aveva quando salvato per la prima volta, anche se la presentazione digitale cambia (e.g. Word to.pdf)
- Se il contenuto presentato ogni volta è selezionato da un contenuto fisso nel sistema e le regole che governano la selezione non cambiano, ogni presentazione è una vista diversa dello stesso documento immagazzinato (e.g. dati statistici)
- "Variabilità limitata": se le variazioni nella forma sono causate dalla tecnologia o dovute all'intenzione dell'autore e ciò che le permette o causa è anche ciò che le limita

Caratteristiche del documento digitale (cont.)

- **Elementi formali**: le caratteristiche che sono visibili sulla faccia del documento, come l'intestazione, il saluto, la sottoscrizione (elementi intrinseci), o il colore, la punteggiatura, il sigillo (elementi estrinseci)
- **Attributi**: le caratteristiche, come il nome dell'autore, la data o la materia, che gli forniscono un'identità unica. Possono manifestarsi come elementi di forma o come metadati connessi al documento, o possono essere impliciti nei suoi vari contesti (documentario, procedurale, tecnologico, di provenienza, o giuridico-amministrativo)
- **Componenti digitali**: un oggetto digitale che contiene tutto o parte del contenuto di un documento e/o i dati o i metadati necessari a ordinare, strutturare o manifestare il contenuto, e che richiede un metodo specifico di conservazione. Quando il documento viene immagazzinato si scinde nelle sue componenti digitali, che sono perciò unità di conservazione. Il documento digitale non esiste come un'entità fisica dopo essere stato chiuso per la prima volta.

Documenti immagazzinati e manifesti

- **Documento immagazzinato**: le componenti digitali usate nel riprodurre un documento o più di uno, compresi i dati che devono essere elaborati per riprodurre il documento manifesto (dati di contenuto e dati di forma) e le regole per processare i dati, incluse quelle che abilitano le variazioni (dati di composizione)
- **Documento manifesto**: la visualizzazione o materializzazione del documento in una forma appropriata per essere presentato a una persona o un sistema. A volte non c'è un documento immagazzinato che gli corrisponda, ma viene ricreato da dati fissi di contenuto quando l'atto di un utente li associa con dati specifici di forma e composizione (e.g. un documento prodotto da una banca dati relazionale)

Tipologia di documenti digitali

Documento statico: non esiste la possibilitàdi cambiarne il contenuto o la forma manifestati sul monitor e ne è permessa solo l'apertura, la chiusura e la navigazione interna.

Appena un documento statico è reperito e manifestato sul monitor, il suo intero contenuto è disponibile all'utente e la sua struttura è invariabile.

Linterazione dell'utente con il sistema non cambiano il contenuto o la forma del documento.

Richieste identiche di ogni utente che eserciti l'opzione di navigare all'interno del documento o di vedere il documento manifestato in modi diversi ottengono gli stessi risultati

Tipi di documenti statici

Documenti che costituiscono gli equivalenti digitali di documenti tradizionali.

Esempi

Lettere; relazioni su esperimenti scientifici o su osservazioni di fenomeni naturali prodotte da sistemi dinamici; registrazioni digitali di pezzi musicali; film digitale; fotografie digitali.

Tipi di documenti statici (cont.)

Documenti che non trovano un esatto equivalente tra i documenti tradizionali ma hanno forma documentaria fissa e contenuto inalterabile.

Esempi

Presentazioni di pagine web, e registrazioni di esecuzioni di opere d'arte che presentano caratteristiche che possono esistere solo in ambiente digitale; i risultati dell'atto di congelare e di catturare l'output di un sistema che modifica le sue proprie istruzioni per manipolare o presentare contenuti.

Tipologia di documenti digitali (cont.)

Documenti interattivi:

Documenti che presentano contenuto e/o forma variabile ma per i quali le regole che governano il contenuto e la forma della presentazione possono essere o fisse o variabili

Tipi di documenti interattivi

Documenti interattivi che *non sono* dinamici:

Documenti per i quali le regole che governano il contenuto e la forma della presentazione *non* variano, e per i quali il contenuto presentato in ciascun caso è selezionato tra i dati contenuti in un un deposito fisso di dati entro il sistema (=variabilità limitata).

Esempi

- *Cataloghi di vendita online, pagine web interattive, e documenti che permettono l'esecuzione di musica e altre opere d'arte, come computer patches.*

Tipi di documenti interattivi (cont.)

Documenti interattivi che ***sono*** dinamici:

Documenti per i quali le regole che governano il contenuto e la forma della presentazione possono variare

Sottotipi:

1. Documenti per i quali le regole che governano il contenuto della presentazione variano perchè essi includono o sono influenzati da dati che cambiano frequentemente, come

   Documenti in sistemi disegnati in un modo che permette l'aggiornamento, la sostituzione o l'alterazione dei dati ma non il mantenimento dei dati precedenti, e siti web che acquisiscono dati dagli utenti o riguardanti le interazioni degli utenti con il sito o iI loro interventi sul sito, e usano quei dati per generare o per determinare le presentazioni successive.

Documenti interattivi dinamici (cont.)

2. Documenti il cui contenuto varia perchè include dati ricevuti da fonti esterne e non immagazzinati nel sistema, come *Siti web che presentano informazione su soggetti come il tempo o il tasso di cambio della valuta; opere d'arte interattive*
3. Documenti prodotti in applicazioni di "dynamic computing", come Geographic Information Systems, che selezionano gruppi diversi di regole per produrre i documenti sulla base delle variazioni nell'input dell'utente, nelle fonti dei dati che formano il contenuto, e nelle caratteristiche del contenuto stesso

Tipi di documenti interattivi (cont.)

4. Documenti prodotti da “adaptive or evolutionary computing applications”, dove il software che genera i documenti può cambiare autonomamente, come

   Siti web che includono la schedatura e modellatura dei mercati finanziari e alcuni tipi di siti per intrattenimento.

Funzione del documento digitale

- ***Ad substantiam*** and ***ad probationem*** (dispositivi e probativi=documenti legali)
- **Di supporto**: generati per essere usati nel corso di varie attività come fonte di informazione (e.g., GIS)
- **Narrativi**: generati come strumento di comunicazione ma la loro produzione non è richiesta dal sistema giuridico (e.g., e-mails, rapporti, web sites)

Nuove funzioni

- **Istruttivi**: indicano la forma di presentazione di contenuto esterno al documento in questione (e.g., spartiti, copioni, regole manuali di procedura, istruzioni per riempire moduli)
- **Abilitanti**: abilitano esecuzioni artistiche (software patches), transazioni (interacting business applications), la condotta di esperimenti (un workflow prodotto e usato per fare un esperimento, di cui è strumento e residuo), l'analisi di dati di osservazione (interpreting software), etc.

Digital Forensics

Categorizzazione dei documenti digitali:

1. Documenti prodotti e tenuti in un computer
2. Documenti prodotti da un computer o dall'interazione di sistemi
3. Documenti prodotti da una persona fisica e un computer
4. Oggetti dinamici: nell'Internet

I primi sono esaminati e valutati come documenti archivistici (inerentemente affidabili)

I secondi sono esaminati e valutati come ogni prova materiale

I terzi e i quarti devono passare entrambi i test

Un documento degno di fede

Un documento affidabile e autentico

(*in contrasto con la diplomatica classica, che fa coincidere i due concetti, presumendo che il secondo implichi il primo*)

Affidabilità

La capacità di un documento di rappresentare i fatti di cui tratta

(*è la responsabilità del produttore ed è stabilita sulla base della completezza del documento e dei controlli stabiliti sulla procedura che lo produce*)

Autenticità

Si riferisce al fatto che un documento sia ciò che dichiara di essere e non sia stato falsificato o corrotto

(*è a rischio durante la trasmissione e la conservazione, è la responsabilità sia del produttore che dell'archivio, e si stabilisce sulla base del rispetto dei requisiti stabiliti per presumere, verificare o mantenere l'autenticità*)

Accuratezza

- Si riferisce all'esattezza e correttezza del contenuto
- E' la responsabilita' dell'autore e dell'archivista
- Dipende dal controllo sui processi che registrano i dati e che li trasferiscono tra sistemi e nel tempo

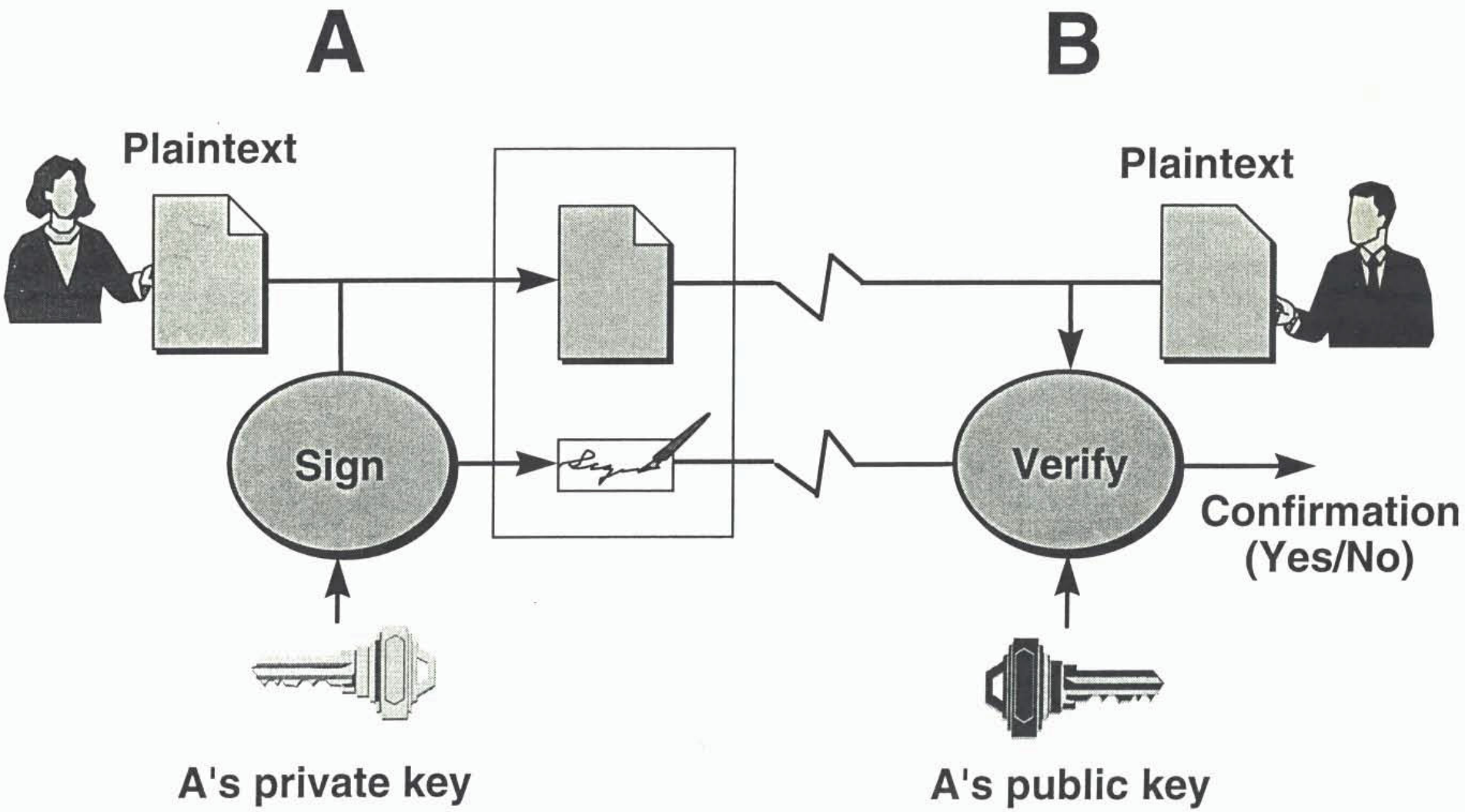
Autenticazione

- Una dichiarazione di autenticità che risulta o dall'inserimento o dall'aggiunta di un elemento o di un'affermazione al documento, secondo norme legislative
- Un metodo per provare che un documento è quello che dichiara di essere in un momento determinato (sigilli, firme digitali)

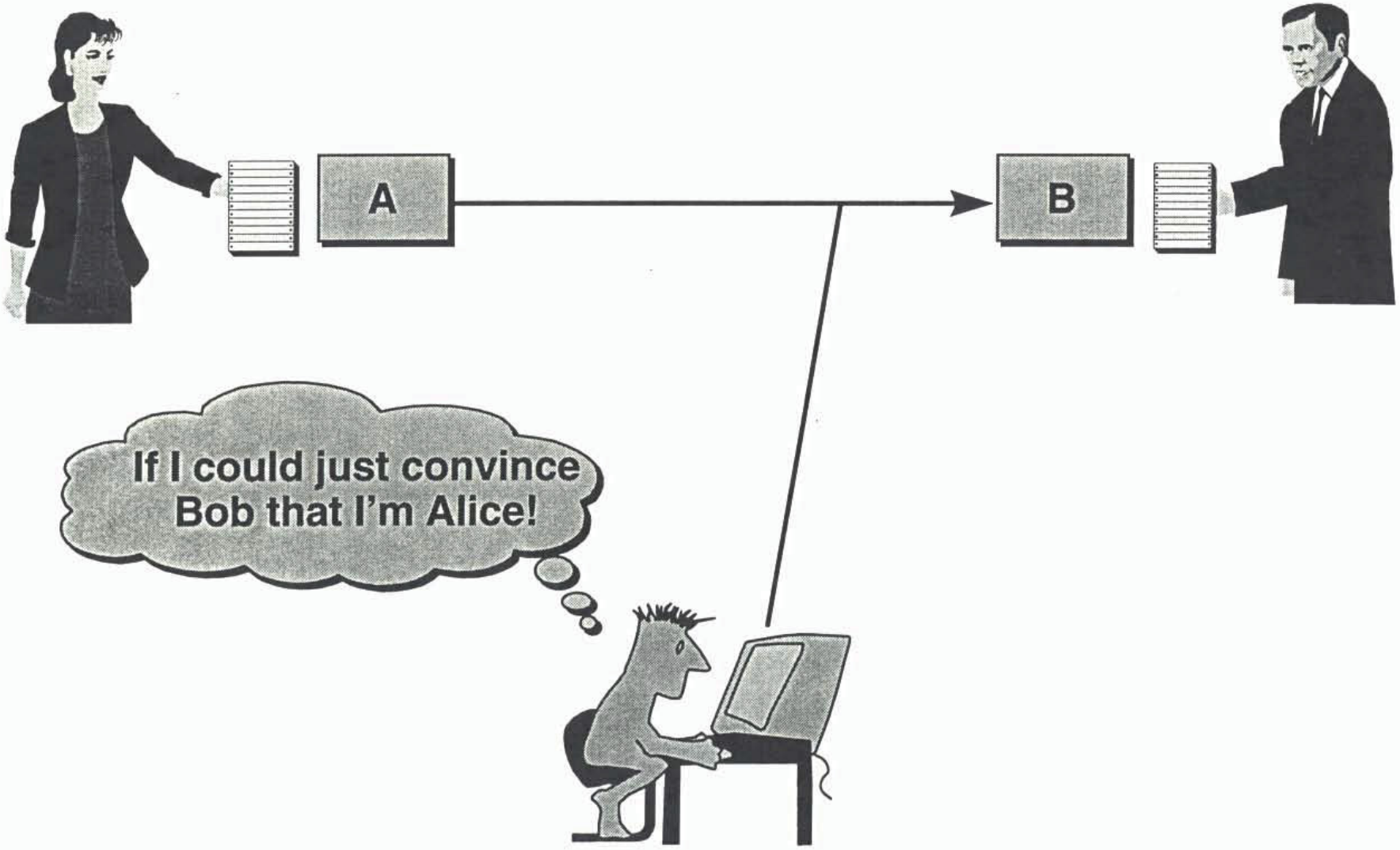
Autenticità e autenticazione

- Certe tecniche matematiche si dice che forniscano un meccanismo **incontrovertibile** per assicurare l'autenticità di oggetti digitali (e.g., firme digitali crittografiche)
- A tali tecnologie si è dato valore legale (e.g., European Directive on electronic signatures, Security and Exchange Commission on hash functions).
- La firma digitale è abilitata da una infrastruttura complessa a chiave pubblica che è molto costosa (PKI)
- La firma digitale è basata sulla stessa tecnica matematica usata dalla cifratura, ma **non** dà confidenzialità

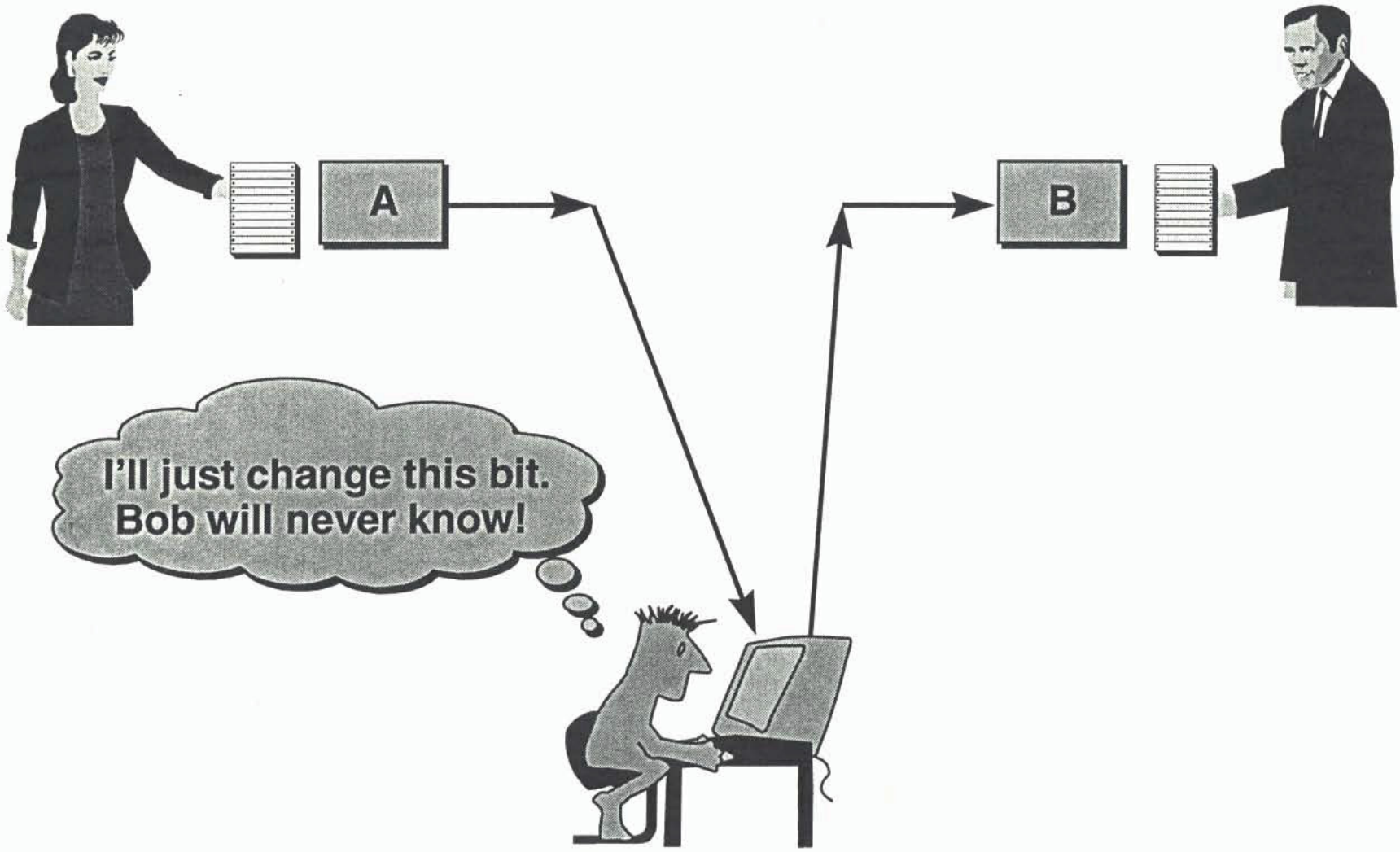
Digital Signature



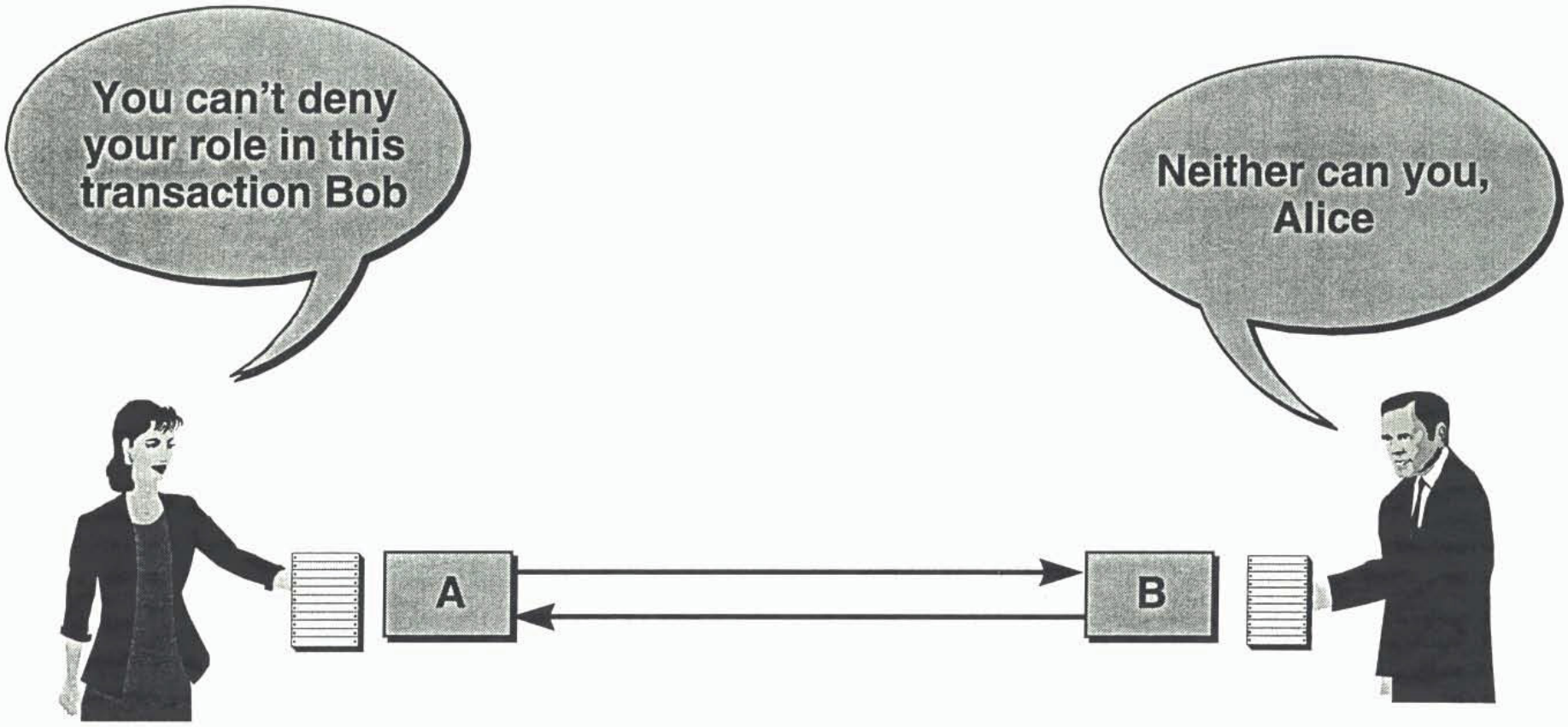
Authentication



Integrity



Non-Repudiation



La firma digitale e la conservazione

- La firma digitale è uno strumento valido per garantire l'autenticità dei documenti attraverso lo **spazio**…
- **…ma non nel tempo**!
- La firma digitale è soggetta a obsolescenza e quindi complica il problema della conservazione digitale
- Gli istituti archivistici nordamericani hanno annunciato che non accetteranno in versamento i documenti cifrati o firmati digitalmente

Autenticità e Autenticazione

- Autenticità è una proprietà del documento che lo accompagna per tutto il tempo che il documento esiste. Si stabilisce sulla base dell'identità e dell'integrità del documento.
- Autenticazione è uno dei modi di provare che un documento è autentico in un momento specifico

Identità di un documento

è costituita dagli attributi di un documento che lo caratterizzano in modo unico e lo distinguono da altri documenti. Questi attributi includono:

i nomi delle persone che concorrono alla sua formazione,
le date di produzione e trasmissione,
la materia o l'atto a cui si riferisce,
la sua forma documentaria e digitale,
l'espressione della sua relazione con gli altri documenti,
l'indicazione di allegati,
il nome dell'ufficio competente,
esistenza di firma digitale.

Integrità di un documento

- La sua interezza e perfezione. Un documento ha integrità se è intatto e non corrotto, cioè se il messaggio che intendeva comunicare per raggiungere il suo scopo è inalterato
- L'integrità fisica di un documento, come per esempio il numero appropriato di bit strings, può essere compromessa, purchè l'articolazione del contenuto e i necessari elementi formali rimangano gli stessi.
- Integrità può essere dimostrata o da evidenza che appare sul documento o da attributi, espressi come metadati, relativi al documento, o in uno o più contesti
- I metadati che la dimostrano sono relativi alla responsabilità per il documento e alle sue trasformazioni technologiche

Attributi di integrità

nome della persona competente per la pratica
nome della persona responsabile per il documento
esistenza di annotazioni
indicazione di cambiamenti tecnici
indicazione di firme digitali aggiunte o rimosse
data della rimozione pianificata dal sistema
data di trasferimento al custode designato
data di distruzione pianificata
esistenza e collocazione di duplicati

Quadro concettuale per i requisiti per l'autenticità

- Con i sistemi elettronici, la presunzione di autenticità deve essere basata su prova che un documento è ciò che dichiara di essere e che non è stato modificato o corrotto in modo sostanziale.
- Per stabilire l'autenticità di un documento, la persona responsabile per la sua conservazione deve poter stabilire la sua identità e dimostrare la sua integrità durante il processo di valutazione per la selezione
- Tale persona assume il ruolo di **custode designato affidabile**

Custode affidabile

Terza parte neutrale: una persona giuridica che è professionalmente competente nell'area di gestione dei documenti, che non ha interesse nel contenuto dei documenti e che agisce come ispettore prima e garante poi

Responsabilità: controllo sul processo di produzione, selezione, conservazione

- In considerazione del fatto che i processi di immagazinamento e reperimento comportano trasformazioni fisiche e di rappresentazione, il concetto tradizionale di conservazione deve essere ampliato e includere i processi necessari ad assicurare la trasmissione inalterata nel tempo del documento
- **La catena ininterrotta di conservazione** comincia col garantire che i documenti siano prodotti in un sistema documentario affidabile e continua con la documentazione di tutti i cambiamenti subiti dai documenti e dei processi di selezione, trasferimento, riproduzione e conservazione

Controllo sul sistema di produzione dei documenti

Un sistema affidabile deve contenere:

1. uno schema di metadati di identità
2. procedure amministrative e documentarie
   integrate in una struttura di workflow
   connessa
   ad uno schema di classificazione e un titolario
3. determinazione di forme documentarie
4. privilegi di accesso a documenti in corso di
   produzione

Controllo sul sistema di tenuta dei documenti

Un sistema affidabile deve contenere:

1. uno schema di metadati di integrità
2. uno schema di classificazione e titolario
3. una scheda di selezione e scarto connessa al titolario
4. un sistema di registrazione
5. un sistema di reperimento
6. previlegi di accesso a documenti archiviati

Digital Forensics: Integrità

Integrità dei documenti: il fatto che non siano modificati intenzionalmente o involontariamente senza l'autorizzazione necessaria

Integrità della riproduzione: il fatto che la produzione di un duplicato non modifichi il documento e che il duplicato sia una copia formalmente esatta del documento riprodotto. Per questo motivo è importante che la riproduzione sia connessa a dati temporali.

Digital Forensics: Integrità

Integrità del computer: il computer produce risultati accurati quando viene usato e oprato in modo appropriato e fu usato in tal modo quando il documento fu prodotto

Integrità del sistema: il sistema ha esercitato le sue funzioni in modo appropriato, senza manipolazioni o intenzionali o involontarie

Regole per stabilire l'integrità di computer e sistema

La teoria, la procedura o il processo per produrre o gestire e mantenere il documento

- Devono essere stati testati e non possono essere stati manomessi
- Devono essere stati sottoposti alla valutazione di esperti e/o sono risultati in pubblicazione (e.g. standards)
- Devono essere generalmente accettati dalla comunità scientifica competente, e
- La ratio di errore conosciuta o potenziale che offrono deve essere accettabile

Il sistema migliore

- Gli attributi di tale sistema sono **ripetibilità delle operazioni, verificabilità, oggettività e trasparenza,** che richiedono la documentazione accurata di qualunque operazione sul sistema e all'interno del sistema.

- **Open source software** è la scelta migliore per valutare integrità, specialmente in caso di upgrade, conversione e migrazione, perchè permette la dimostrazione pratica che niente puo' essere alterato, perso, piantato o distrutto volontariamente o inavvertitamente

Principi relativi all'integrità

Non-interferenza: il metodo usato per fare upgrade, conversion o migration non cambia il contenuto e la forma documentaria del documento nativo

Interferenza identificabile: il metodo usato per fare upgrade, conversion o migration altera il documento nativo ma i cambiamenti sono identificabili

Questi principi, che incorporano la posizione etica e professionale dell'archivista, caratterizzano anche il suo ruolo istituzionale di custode affidabile che esercita il controllo sul sistema di produzione e gestione dei documenti

Principi relativi all'autenticita'

- **Autenticità** è la certezza dell'identità della fonte, persona o sistema. Autenticità implica integrità ma non viceversa.
- Autenticità si puo' basare sulla dichiarazione di un esperto che il sistema di gestione e tenuta dei documenti e le procedure che lo controllano sono affidabili, sulla base di
    1. uno schema di metadati di identità e integrità
    2. uno schema di classificazione (titolario)
    3. regole di selezione e scarto connesse al titolario
    4. un sistema di registrazione di protocollo
    5. un sistema di reperimento
    6. previlegi di accesso a documenti archiviati

Autenticazione

- La firma digitale è uno strumento valido per garantire l'autenticità dei documenti attraverso lo **spazio……ma non nel tempo**!
- I sistemi giuridici nordamericani non la considerano il miglior metodo di autenticazione
- La firma digitale è soggetta a obsolescenza e quindi complica il problema della conservazione digitale
- Il metodo prevalente di autenticazione è **una catena di custodia legittima** in sistemi che passino i test di **ripetibilità, verificabilità, oggettività e trasparenza.**

E in assenza di catena di custodia legittima?

Questa **Catena Ininterrotta di Custodia** (vedi InterPARES COP model) è possibile—almeno in teoria– per i documenti digitali di istituti e enti pubblici e privati per cui esiste un'entità archivio designata esterna (ministero, tribunale) o interna (università, banca).

Come conservare i documenti digitali per cui non esiste un archivio storico designato?

Parliamo di archivi di professionisti, persone, famiglie, studi (architetti, avvocati, dentisti), ditte, ecc.

Due situazioni possibili

1. La sovrintendenza o l'archivio storico interviene quando i documenti sono ancora correnti e
    1. il produttore desidera collaborazione
    2. Il produttore accetta consigli anche se senza interferenza
2. La sovrintendenza o l'archivio storico si trova di fronte a documenti non correnti, spesso su supporti esterni al sistema in cui sono stati prodotti

Situazione di collaborazione

a) Creare un' infrastruttura

- stabilire la portata e gli obbiettivi
- acquisire risorse
- focus sui documenti digitali
- dare consiglio su tecnologia e formati
- fornire esempi
- sviluppare policy e procedure, assegnare responsabilità
- sviluppare strategie di mantenimento

Collaborazione

b) Valutare i documenti

- Identificare i documenti tra gli oggetti digitali prodotti
- Identificare co-autori e proprietari multipli
- Determinare l'autenticità e documentarla
- Determinare problemi di privacy
- Monitorare i documenti da conservare
- Identificare tutte le componenti digitali
- Determinare la fattibilità della conservazione
- Sviluppare un piano di versamento

Collaborazione

c) Versamento

- Migrare i documenti all'ambiente tecnologico dell'archivio
- Conservare il formato logico più vecchio ancora disponibile
- Evitare l'acquisizione di duplicati
- Documentare ogni attività a cui i documenti sono sottoposti

Consigli senza interferenza

Si preparano linee guida chiare e comprensibili

- Un opuscolo generale
  - Come scegliere software e formati (standards)
  - Come organizzare i documenti
  - Come mantenere i documenti accessibili nel tempo (back-ups, system upgrade, conversione, dispersione)
  - Come prevenire la perdita di documenti

Cont.

Consigli senza interferenza

- **Un opuscolo specifico sulla gestione e tenuta dell'e-mail**
  - Come organizzarla, anche in relazione ad altri documenti
  - Come trattare gli attachments
  - Come trattare I threads
  - Come conservarla in altri formati
  - Come selezionarla
- **Un opuscolo su come donare i propri documenti digitali**
  - Perchè donare, cosa donare, come, quando
  - Considerazioni sui diritti intellettualy, di privacy, sicurezza, accesso
  - Lista di persone/enti a cui rivolgersi per consigli e aiuto
- **Lezioni e workshops su come proteggere le proprie foto, ecc**.

Assenza di contatto

Materiali che ci potrebbero essere presentati:

- **Documenti generati da word processing**
- **E-mail con word processing attachments**
- **Foto, video e registrazioni musicali**
- **Agende o calendari**
- **Web portals, blogs & wikis**
- **Registrazioni di videoconferenze & webcasting**
- **Databases**
- **Flash drives & altre storage devices con contenuti vari**
- **Remote PDAs, Blackberrys, etc. etc. etc.**

Assenza di contatto

Siamo di fronte a oggetti digitali non correnti, spesso su supporti esterni al sistema in cui sono stati prodotti

Regole da seguire:

- Si crea una copia o un'immagine (non sono la stessa cosa)
- Si analizza la copia o l'immagine e si determina se gli oggetti digitali sono documenti
- Se sono documenti, si determina la loro autenticità
- Si determina la fattibilità della conservazione
- Si procede al versamento

Il processo di Digital Forensics

1. Produzione della copia delle entità logiche o dell'immagine dell'hard drive o supporto esterno
2. Identificazione degli oggetti di interesse potenziale
3. Analisi degli oggetti identificati
4. Valutazione e interpretazione dei risultati
5. Presentazione dei risultati in un rapporto che descrive in dettaglio le caratteristiche degli oggetti, l'interpretazione dei fatti e le opinioni di esperti
6. La revisione tecnica e amministrativa da parte di un soggetto neutrale

Trasferimento all'archivio storico

Le procedure e i sistemi usati per trasferire i documenti all'archivio storico, mantenerli e riprodurli devono incorporare controlli adeguati e efficaci per garantire l'identità e l'integrità dei documenti, e specificatamente devono assicurare che:

- Sia mantenuta la custodia ininterrotta dei documenti;
- Siano rispettate regole relative a metadati, privilegi di accesso
- Siano messe in atto e monitorate procedure di protezione, sicurezza e controllo; e
- Il contenuto dei documenti rimanga inalterato dopo la riproduzione

Conservazione

- Non è possible conservare un documento elettronico, ma solo la capacità di riprodurlo. Perciò dobbiamo proteggere le componenti digitali che contengono la sostanza delle parti costitutive e dell'identità del documento.
- Dobbiamo accettare che è impossibile mantenere letteralmente inalterato un documento elettronico
- L'unico modo di provare che un documento elettronico è autentico è produrre una copia autentica dei documenti del produttore presunti o verificati autentici

Documentazione della riproduzione

L'attività di riproduzione deve essere documentata e la documentazione deve includere:

- La data della riproduzione e il nome della persona responsabile;
- Una descrizione della relazione tra i documenti acquisiti dal produttore e le copie prodotte dall'archivista;
- Una descrizione dell'impatto del processo di riproduzione sulla forma, il contenuto, l'accessibilità e l'uso dei documenti; e
- Nei casi in cui la copia non riproduca pienamente e fedelmente gli elementi che esprimono l'identità e integrità del documento, tale informazione deve essere documentata dall'archivista e questa documentazione deve essere facilmente accessibile all'utente.

Mantenere sempre il formato nativo

Descrizione archivistica

La descrizione archivistica del fondo che contiene i documenti elettronici deve includere—oltre all'informazione sui contesti giuridico-amministrativo, di provenienza, procedurale e documentario—anche informazione sui cambiamenti che i documenti hanno subito fin da quando sono stati prodotti

Conservazione affidabile

L'autenticità delle copie prodotte dall'archivista è garantita da:

- Un processo controllato di migrazione all'ambiente tecnologico dell'archivio
- La documentazione accurata di ogni cambiamento durante il processo e successivi "upgrades"
- Lo stabilimento e il monitoraggio di privilegi di accesso, uso e riproduzione in archivio

Conservazione affidabile (cont.)

- Lo stabilimento di procedure per **prevenire**, **scoprire**, e **correggere** la perdita o la corruzione dei documenti
- Lo stabilimento di procedure per garantire l'identità e l'integrità dei documenti attraverso il deterioramento dei supporti e l'obsolescenza tecnologica
- La determinazione dei modi di autenticazione e delle responsabilità per l'autenticazione

Conservazione affidabile

- La fonte più importante per stabilire l'autenticità dei documenti è la descrizione archivistica
- Descrizione come attestazione collettiva dell'autenticità dei documenti in un fondo e di tutte le loro relazioni
- Descrizione come prospettiva storica sui documenti e sulle loro trasformazioni

Linee guida per la conservazione: 1. infrastruttura

1.1 stabilire il raggio e gli obbiettivi
1.2 acquisire risorse
1.3 focus sui documenti digitali
1.4 dare consiglio
1.5 dare il buon esempio
1.6 sviluppare procedure
1.7 implemetare strategie di mantenimento

2. Valutare e selezionare i documenti

2.1 Valutare presto
2.2 Identificare proprietari multipli
2.3 Determinare l'autenticità
2.4 Documentare la determinazione di autenticità
2.5 Monitorare i documenti da conservare
2.6 Aggiornare la valutazione
2.7 Identificare tutte le componenti digitali
2.8 Determinare la fattibilità della conservazione

3. Acquisire i documenti selezionati

3.1 Sviluppare piani di versamento concordati
3.2 Implementare procedure standardizzate
3.3 Conservare il formato logico più vecchio ancora disponibile
3.4 Evitare l'acquisizione di duplicati
3.5 Documentare ogni attività a cui i documenti sono sottoposti

4. Conservare i documenti acquisiti

4.1 Descrivere i documenti
4.2 Identificare le ramificazioni legali di attività di conservazione
4.3 Confermare la validità e efficacia della strategia di conservazione prescelta
4.4 Mantenere un ambiente fisico di conservazione appropriato per il materiale

5. Facilitare l'accesso ai documenti

5.1 Spiegare come le copie per la consultazione sono prodotte

5.2 Spiegare i requisiti tecnici che permettono l'accesso

Strategie di conservazione
1. Uso di standards

De iure standards versus de facto standards

1.1 Formati che si autodescrivono
1.2 Incapsulamento
1.3 Limitare il raggio di formati da gestire
1.4 Conversione

Strategie di conservazione
2. Dipendenza tecnologica

2.1 Conservare la tecnologia
2.2 Affidarsi alla compatibilità con versioni precedenti
2.3 Trasformare il software
2.4 Conversione al momento di accesso
2.5 Emulazione
2.6 Approccio non digitale
2.7 Archeologia digitale

La triste realtà

La maggior parte dei sistemi che dovrebbero contenere documenti contengono solo dati, perchè le entità che essi producono non hanno forma fissa e contenuto stabile. Quando un sistema contiene documenti, il loro contesto amministrativo e documentario non è identificabile.

I documenti non correnti che non sono mantenuti in sistemi attivi spesso non possono essere conservati perchè o sono stati prodotti o mantenuti in formati non conservabili o sono obsoleti.

Lezioni da ricordare

La conservazione di documenti digitali autentici

- è un processo continuo che comincia con la produzione dei documenti
- deve essere basata sui concetti di sistema affidabile di tenuta dei documenti e sul ruolo dell'archivista come custode di fiducia
- deve incorporare la selezione dei documenti e la descrizione archivistica

Lezioni da ricordare

- Il solo modo di conservare un documento non corrente è fare una copia autentica della sua ultima manifestazione come documento autentico del produttore
- L'archivista deve essere competente sia per la valutazione che per il mantenimento dell'autenticità dei documenti elettronici durante il loro intero ciclo vitale

Lezioni da ricordare

- Le soluzioni al problema della conservazione digitale sono dinamiche a causa dell'evoluzione continua della tecnologia e dell'aumento della sua complessità
- La tecnologia non può determinare la soluzione alla conservazione nei tempi lunghi dei documenti digitali
- I requisiti archivistici devono definire il problema e i principi archivistici devono stabilire la correttezza e l'adeguatezza di ogni soluzione tecnica

Web Sites

www.digitalrecordsforensics.org

www.interpares.org