La PEC: i rischi specifici e i sistemi omologhi all'estero

Le garanzie della PEC

Il punto di vista legale: quali sono gli obiettivi prefissi?

- Validità legale della trasmissione
- "garantisce la provenienza, l'integrità e l'autenticità del messaggio di posta elettronica certificata secondo le modalità previste dalle regole tecniche"
  - *l'autenticità?* Forse in riferimento al Punto di Ricezione...
- L'identificazione del titolare è facoltativa e ha un valore normato solo nel caso di trasmissioni da un cittadino alla Pubblica Amministrazione

Equivalenza alla raccomandata

- La trasmissione è "valida agli effetti di legge"
- La data e l'ora sono "opponibili a terzi"

Mezzi tecnici per la garanzia

- La PEC si avvale della "firma elettronica avanzata"
- Non è obbligatorio avvalersi di dispositivi sicuri per la creazione della firma
- Aspetto legale: fino a quando le notifiche firmate dal gestore sono legalmente valide?
  Bisogna apporre una marca temporale?

Falsificazione di un messaggio PEC

- I gestori PEC devono conservare i log relativi all'elaborazione dei messaggi transitati per trenta mesi
  - Il diritto di accedervi è garantito, ma non è chiaro a chi, né con quali modalità
- In molti scenari, per l'"attaccante" può essere sufficiente che il messaggio compaia nella casella del destinatario
- Chi consulta la propria casella PEC su un sistema adeguatamente sicuro?

Falsificazione di un messaggio PEC

- Per facilitare l'utilizzo della PEC, i gestori firmano i messaggi con certificati emessi da una sub-CA che a sua volta è garantita da una CA largamente riconosciuta

- Perché i MUA (i programmi per la lettura e la gestione della posta) siano contenti, è sufficiente che il certificato sia considerato valido nell'ambiente in cui il messaggio viene letto

Falsificazione di una ricevuta

- La ricevuta di consegna può essere validamente prodotta per dimostrare un'avvenuta trasmissione
- Per generare una firma valida, è necessario
  - disporre della chiave privata di firma elettronica avanzata del gestore destinatario
  - oppure generare dei dati accettabili da parte del sistema che dovrà verificare la validità della firma

Falsificazione di una ricevuta

- Il rischio di compromissione della chiave privata (dati di creazione della firma) dipende
  - dalle misure adottate dal gestore
  - dalla bontà del sistema adottato per generare tali dati

La validità della consegna

- Dal momento in cui il gestore PEC del destinatario consegna il messaggio nella casella, non sussistono obblighi in capo ad esso
  - la normativa non impone espressamente la tracciabilità degli accessi alla casella
- Che cosa succede se un terzo non autorizzato cancella un messaggio ricevuto?

Il riconoscimento tra gestori PEC

- È basato sulla consultazione di una copia dell'IGPEC, l'Indice dei Gestori
- Ogni gestore mette a disposizione del sistema centrale, via HTTPS, un file in formato LDIF con i dati da esibire
- Il sistema centrale li raccoglie, li verifica e mette l'indice a disposizione dei singoli gestori

Sistemi progettati all'estero

- ETSI, ente per la standardizzazione riconosciuto dall'ordinamento UE, ha un comitato tecnico per le "Electronic Signatures and Infrastructures" (ESI)

- Nel 2007 ha ultimato un'indagine volta a conoscere lo stato dell'arte della "Registered Electronic Mail" ("posta elettronica raccomandata") in Europa, illustrata nel TR 102 605

AUSTRIA: CONSEGNA ELETTRONICA

- Le persone fisiche e giuridiche possono scegliere di ricevere documenti dalla P.A. per via elettronica
  - Si registrano presso un fornitore autorizzato, che li include in un elenco statale
  - Quando devono ricevere un documento, ricevono fino a due notifiche elettroniche ed una terza cartacea, se necessaria
  - Se è richiesta una prova di consegna, la notifica non include il documento, ma dà la possibilità di scaricarlo

AUSTRIA: CONSEGNA ELETTRONICA

- Le P.A. dispongono di un unico servizio di consegna, che si incarica di portarla a termine in modo elettronico, se possibile, o cartaceo altrimenti

SPAGNA: UPM-ACEPTA

- È un servizio sviluppato dal Politecnico di Madrid, ma non implementato
- Il mittente cifra la comunicazione con una chiave *k* composta da due metà, *k1* e *k2*
- Il mittente invia la comunicazione al destinatario insieme a *k1*; invia invece *k2*, insieme ai dati del destinatario, al gestore abilitato

SPAGNA: UPM-ACEPTA

- Il destinatario dimostra il possesso della comunicazione al gestore, e riceve da esso la chiave *k2* per poterla leggere

Lo standard REM

- È uno standard ETSI (TS 102 640, v. 2.2.1)
- È nato per poter garantire l'interoperabilità tra vari gestori e vari sistemi di REM
- Il singolo gestore, chiamato REM-MD (Management Domain), fa parte di un sistema REM autonomo, detto REM-PD (Policy Domain)
- Esempio:
  - Un singolo gestore PEC è un REM-MD
  - Il sistema PEC italiano è un REM-PD

Lo standard REM

- Lo standard definisce la struttura dei messaggi scambiati e prevede che si possano utilizzare sia SMTP che altri protocolli

- Ciascun Policy Domain decide in autonomia come gestire il reciproco riconoscimento tra i vari Management Domain al suo interno

Lo standard REM

Può operare in due modalità:

- Store and Forward (come la PEC)
- Store and Notify: il destinatario riceve istruzioni per scaricare la comunicazione archiviata presso il MD del mittente

Lo standard REM

- È previsto il riconoscimento tra diversi Policy Domain mediante le Trust-service Status List (TSL)
- Un PD che non è interessato ad operare con altri, può adottare meccanismi diversi dalle TSL
- Un PD che desidera operare con altri PD può includere i riferimenti alle loro TSL, o è possibile ricorrere a un sistema gerarchico