Dipartimento Matematica – Facoltà di Scienze
Università degli Studi di Trento

Introduzione alla Posta Elettronica Certificata (PEC): le regole tecniche

Dott. Enrico Zimuel – Secure Software Engineer

http://www.zimuel.it - email: enrico@zimuel.it

Introduzione alla PEC

- Posta elettronica certificata (PEC): è un messaggio di posta elettronica con lo stesso valore legale di una raccomandata con avviso di ricevimento tradizionale
- Regole tecniche:
  - Decreto Ministeriale 2 novembre 2005 [1], G.U. 15 novembre 2005, n. 266
  - DigitPa, ente nazionale per la digitalizzazione della Pubblica Amministrazione (http://www.digitpa.gov.it/)

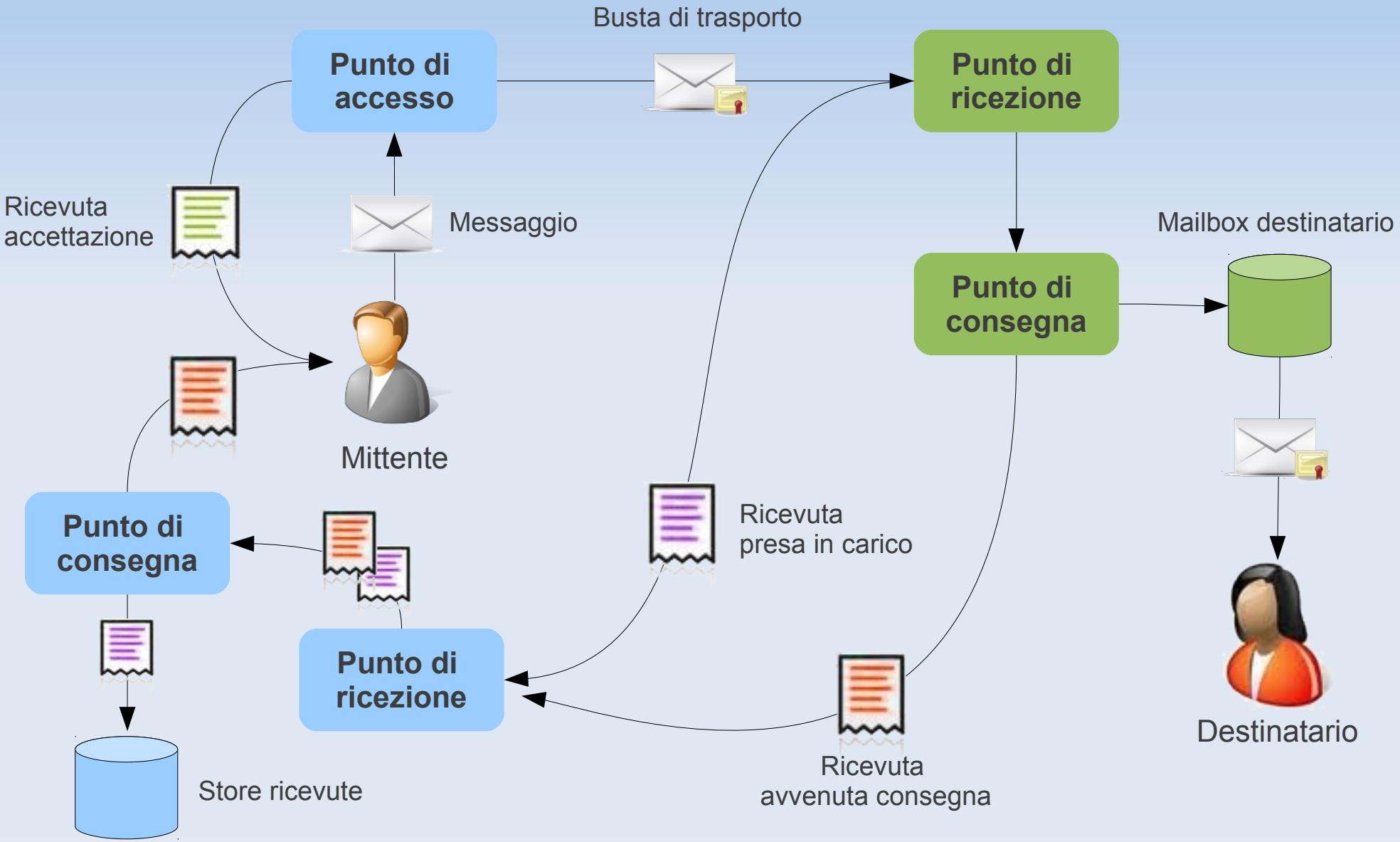
Regole tecniche

- Alcune definizioni:
  - **Punto di accesso**: il sistema che fornisce i servizi di accesso per l'invio e la lettura dei messaggi PEC
  - **Punto di ricezione**: il sistema che riceve il messaggio all'interno di un dominio PEC
  - **Punto di consegna**: il sistema che compie la consegna del messaggio nella casella PEC del titolare destinatario

Regole tecniche (2)

- Alcune definizioni:
  - **Busta di trasporto**: la busta creata dal punto di accesso e sottoscritta con la firma del gestore di posta elettronica certificata mittente, all'interno della quale sono inseriti il messaggio originale inviato dall'utente di posta elettronica certificata ed i relativi dati di certificazione
  - **Marca temporale:** un'evidenza informatica con cui si attribuisce, ad uno o più documenti informatici, un riferimento temporale opponibile ai terzi (DPR 28 dicembre 2000, n. 445, DPCM 13 gennaio 2004)

Schema di funzionamento



Messaggi PEC

- Il sistema di PEC genera i messaggi (ricevute, avvisi e buste) in formato MIME
- I messaggi sono composti da una parte di testo descrittivo, per l'utente, e da una serie di allegati
- Il messaggio è inserito in una struttura S/MIME v3 in formato CMS, firmata con la chiave privata del gestore di posta certificata
- Il certificato associato alla chiave usata per la firma è incluso in tale struttura

Messaggi PEC (2)

- Il formato S/MIME usato per la firma dei messaggi generati dal sistema è il “multipart/signed” (formato .p7s) così come descritto nella RFC 2633 [2]
- I messaggi sono trasferiti tra gestori usando una codifica a 7 bit sia per gli header sia per il corpo del messaggio e gli eventuali allegati (Base64)
- Certificati in standard X.509v3

Mittente del messaggio

- Per garantire la verificabilità della firma da parte del client di posta ricevente, il mittente del messaggio deve coincidere con quello specificato all'interno del certificato usato per la firma S/MIME.
- Msg. originale:
  - From: "Mario Bianchi" <mario.bianchi@dominio.it>
- Busta trasporto:
  - From: "Per conto di: mario.bianchi@dominio.it" <posta-certificata@gestore.it>
  - Reply-To: "Mario Bianchi" <mario.bianchi@dominio.it>

Controlli formali sui messaggi

- Il punto di accesso deve garantire:
  - nel corpo del messaggio esista un campo “From” riportante un indirizzo email conforme alle specifiche RFC 2822
  - nel corpo del messaggio esista un campo “To” riportante uno o più indirizzi email conformi alle specifiche RFC
  - l’indirizzo del mittente del messaggio specificato nei dati di instradamento (reverse path) coincida con quanto specificato nel campo “From” del messaggio

Controlli formali sui messaggi (2)

- gli indirizzi dei destinatari del messaggio specificati nei dati di instradamento (forward path) coincidano con quelli presenti nei campi “To” o “Cc” del messaggio
- non siano presenti indirizzi dei destinatari del messaggio specificati nel campo “Ccn” del messaggio.

Punto di ricezione

- Lo scambio di messaggi tra diversi gestori avviene tramite una transazione basata sul protocollo SMTP come definito dalla RFC 2821 [3]
- Sicurezza:
  - SMTP su trasporto TLS
  - Il punto di ricezione deve prevedere ed annunciare il supporto per l'estensione STARTTLS ed accettare connessioni sia in chiaro (per la posta ordinaria) che su canale protetto

Log

- Tutte le attività sono memorizzate su un registro riportante i dati significativi dell'operazione:
  - il codice identificativo univoco assegnato al messaggio originale
  - la data e l'ora dell'evento
  - il mittente del messaggio originale
  - i destinatari del messaggio originale
  - l'oggetto del messaggio originale
  - il tipo di evento (accettazione, ricezione, consegna, emissione ricevute, errore, ecc.)
  - il codice identificativo (Message-ID) dei messaggi correlati generati (ricevute, errori, ecc.)
  - il gestore mittente

Sicurezza (?) della PEC

- La PEC garantisce soltanto l'avvenuta consegna
  - Non è garantita l'integrità del contenuto
  - Non è garantita l'identità del mittente
  - Non è garantita la privacy del contenuto
- Firma digitale + PEC
  - Garantisco l'integrità del contenuto
  - Garantisco l'identità del mittente
- Encryption + PEC
  - Garantisco la privacy del contenuto

Sicurezza (?) della PEC (2)

- Virus informatici
  - I messaggi PEC devono essere analizzati da un sistema antivirus che deve essere costantemente aggiornato
- La conservazione per 30 mesi delle ricevute includono anche l'intero messaggio e suoi eventuali allegati che sono in chiaro
  - Cosa accade dopo i 30 mesi?
  - Il gestore PEC è l'unico ad avere le credenziali per aprire "la busta di trasporto" con tutto il suo contenuto

Riferimenti

(1) Decreto Ministeriale 2 novembre 2005. *Regole tecniche del servizio di trasmissione di documenti informatici mediante posta elettronica certificata*

(2) RFC 2633, *S/MIME Version 3 Message Specification*

(3) RFC 2821, *Simple Mail Transfer Protocol*

(4) RFC 6109, *La Posta Elettronica Certificata - Italian Certified Electronic Mail*

(5) DigitPA, *Minigrafia - La Posta Elettronica Certificata*

(6) Emilio Robotti, *La PEC, Posta Elettronica Certificata*, Altalex eBook "Informatica Giuridica" (2010)

(7) Massimo F. Penco, *La posta elettronica: tecnica & best practice,* Edisef (2010)