EVOLUZIONE DELLA PEC E PROSPETTIVE IN AMBITO INTERNAZIONALE

Francesco Gennai

Francesco.gennai@isti.cnr.it

CENTRO TECNOLOGICO SERVIZI INTERNET (ISTC)

- Centro Tecnologico Servizi Internet (ISTC)
  - Evoluzione storica a partire dalla prima metà degli anni ’90
    - Gateway tra diverse architetture di email
    - Soluzioni pionieristiche per l’email Internet
  - Integrated Network Services Manager
    - 35 istituti (o sezioni) del Consiglio Nazionale delle Ricerche
      - MailboxManager, ListManager, DnsManager, DhcpManager, WntManager, IdentityManager
  - Infrastrutture di rete wireless (Pisa, Avellino, Napoli, Perugia)
  - Collaborazioni con enti pubblici e con aziende
  - Esperienza nella gestione di progetti
  - Attività di sviluppo

PIATTAFORMA ISTI-PEC

- La piattaforma ISTI – PEC (2005)
  - Sviluppata presso il centro ISTC dell'ISTI
  - Gestione multi-domain-mixed
    - Un stesso server può gestire contemporaneamente:
      - più domini (mailbox) PEC
      - più domini (mailbox) "standard" (non-PEC)
  - Sistema composto da uno o più nodi connessi in cluster
  - Gestione Remote PEC Access/Delivery
    - Per ciascun dominio PEC può gestire uno più punti di accesso/consegna remoti costituiti da un normale server "standard" Internet (cioè non occorre l'installazione di alcun modulo software PEC) (Esempio: server Postfix)
      - Elevata scalabilità della soluzione
      - Estrema flessibilità nella delega dell'amministrazione del dominio PEC

ACCORDO DI COLLABORAZIONE TRA DIGITPA E ISTI - CNR

- Accordo tra DigitPA e ISTI (2008)
  - Test di interoperabilità
  - Revisione delle specifiche
  - Attività internazionali

TEST DI INTEROPERABILITÀ

- Test di interoperabilità
  - Eseguiti tra piattaforma ISTI – PEC e piattaforma del provider
  - 228
  - Durata 10 giorni lavorativi
- A cosa servono
  - Verifica dell'interoperabilità:
    - Verifica della conformità alle Regole Tecniche PEC della piattaforma sotto test
  - Permettono di rilevare problemi nell'interpretazione delle Regole Tecniche
  - Sono fondamentali per il mantenimento di una elevata qualità del servizio PEC nazionale

ATTIVITÀ INTERNAZIONALE DIGITPA / ISTI - CNR

- Attività internazionale
  - Comitati di standardizzazione IETF, IEEE, ANSI ..
  - Internet Engineering Task Force (IETF)
    - Documenti chiamati Request For Comments (RFCnnnn)
- Internet Engineering Task Force (IETF)

  “The mission of the IETF is to make the Internet work better by producing high quality, relevant technical documents that influence the way people design, use, and manage the Internet.”
- Le nostre tappe
  - IETF 71 Philadelphia (marzo 2008) WG S/MIME
  - Pubblicazione RFC 6109 «La Posta Elettronica Certificata - Italian Certified Electronic Mail» (aprile 2011)
  - (Informational)
  - IETF 83 Parigi (martzo 2012) WG APPSAWG

ATTIVITÀ INTERNAZIONALE DIGITPA / ISTI - CNR

- Prossima tappa
  - Messaging Anti-Abuse WG
    - Berlino, 6 – 7 giugno 2012
  - Apple Inc La Caixa AT&T Message Bus Cloudmark, Inc. PayPal Comcast Return Path, Inc. Cox Communications Time Warner Cable Damballa, Inc. Verizon Communications Facebook Yahoo! Inc. France Telecom

SCENARIO INTERNAZIONALE

	Transport Protocol		Message Protocol	
	HTTP	SMTP	SOAP	eMail
PEC (Italy) [RFC6109]		X		X
DeMail (Germany)		X		X
DDS (Austria)	X		X	
Rpost Registered Email (USA)		X		X
Moja.posta.si (SI Post - Slovenia)	X		X	
PosteCS (Canada Post)	X		X	
ERV (Austria)	X		X	
REM (ETSI)		X		X
PReM (Universal Postal Union)	X		X	

None of them is compatible with the others. There are a lot of other examples:
PostX (USA), **Goodmail**, **Tumbleweed**, **E-Postbrief** (Germany), **IncaMail** (Switzerland), **Apartado Postal Electronico** (Spain), **Certipost** (Belgium), **EuroNot@ries eWitness** (EU Notaries), **eNotarius eNmail** (Norway), **Certimail** (Spain), **EGVP** (Germany), **JUBES** (Netherland), **Notificaciones Electronicas** (Spain), **PRESTO** (France), **OCSI** (Germany) ...

EVOLUZIONE DI UN SISTEMA CEM

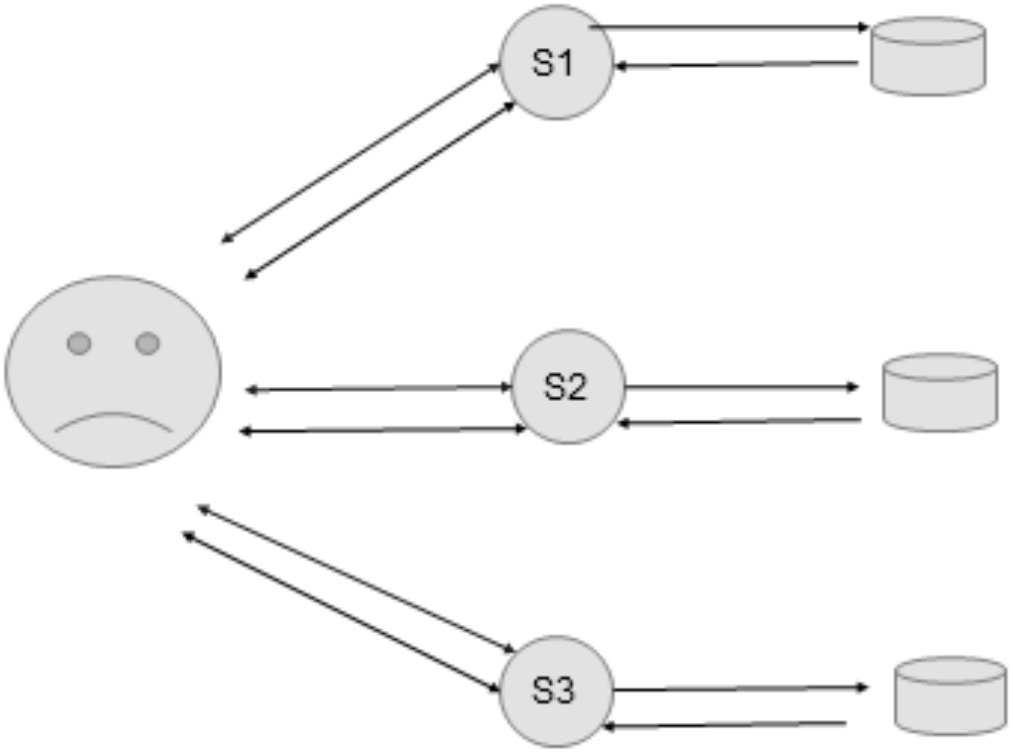
- Evoluzione *interna*
  - Evoluzione delle tecnologie di base
  - Nuove esigenze
- Evoluzione *esterna*
  - Interesse ad operare oltre i confini nazionali
    - Interoperabilità con altre architetture CEM
    - Standard internazionale

TECNOLOGIE INTERNET E PEC

- Gestione degli accessi al servizio: identificazione dell'utente
  - Interfaccia tra *sistema PEC* ed utente
  - Identificazione di un utente (autenticazione mediante credenziali di accesso)
  - Sistemi di Identity Management
  - Evoluzione: mantenere un elevato livello di fruibilità del servizio da parte dell'utente
- Gestione dei domini PEC
  - Interna al *sistema PEC*
  - Certificato del provider associato al dominio mediante sistema LDAP
    - Unico file di testo
  - DNS-Based Authentication of Named Entities
  - Evoluzione: mantenere un elevata affidabilità e operatività del servizio PEC

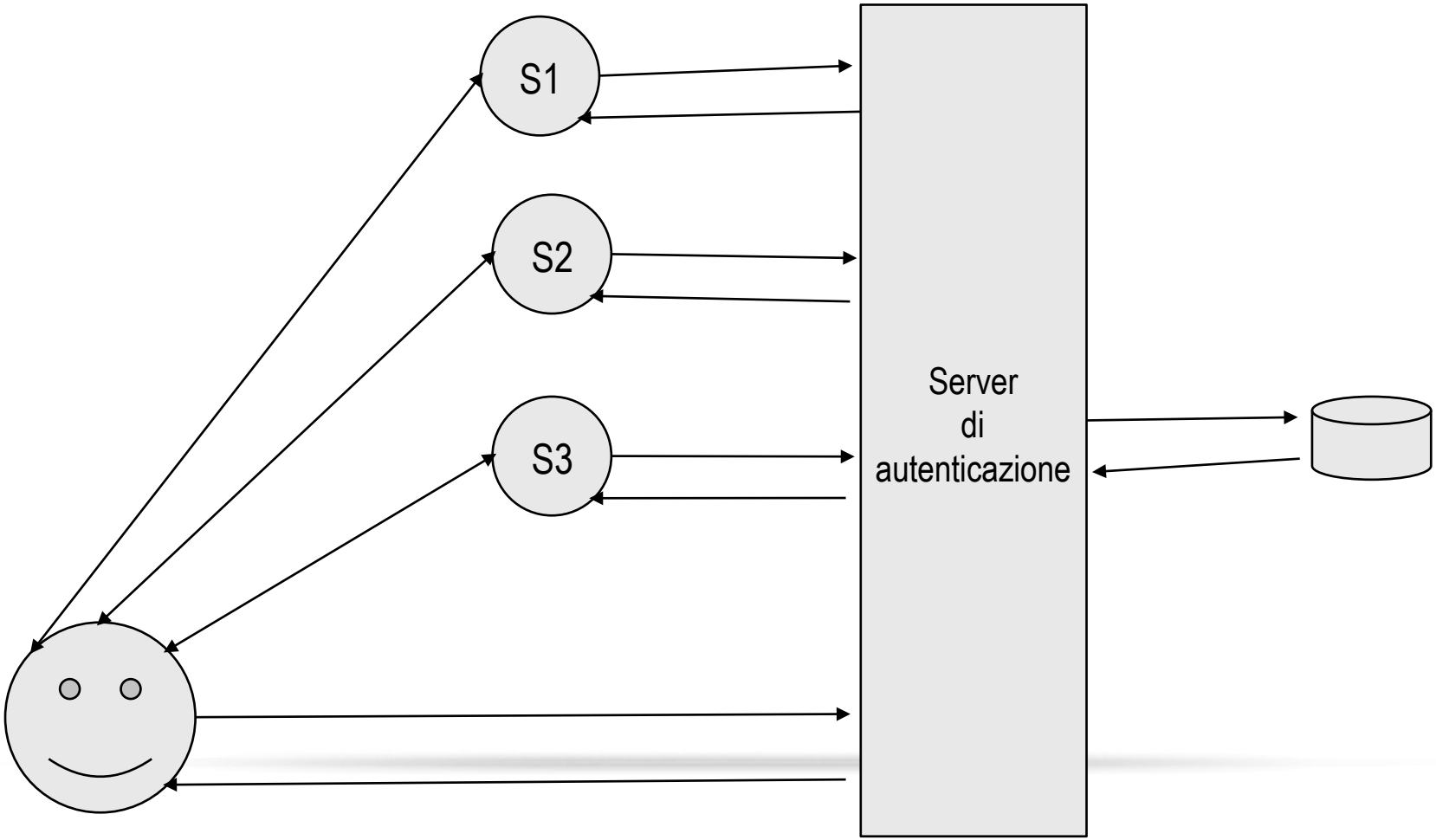
TECNOLOGIE INTERNET E PEC

Autenticazione e autorizzazione



TECNOLOGIE INTERNET E PEC

Autenticazione e autorizzazione



TECNOLOGIE INTERNET E PEC

- Il processo di identificazione di un utente può essere visto come un processo indipendente dal servizio che l'utente vuole accedere
  - Tecnologia consolidata per servizi web (server HTTP)
  - Tecnologia emergente (draft IETF) per servizi email (server SMTP, IMAP, POP)

TECNOLOGIE INTERNET E PEC

- Attualmente
  - Sessioni sicure via Transport Layer Security (TLS)
    - Certificati per associare un nome (Esempio: cnr.it) ad una chiave pubblica
    - Certificati emessi emessi da Certification Authority

      Vulnerabile: emissioni di certificati senza controlli
- Nuovo scenario: DNS-Based Authentication of Named Entities
  - Uso di DNSSEC
    - Chiave pubblica associata al dominio all'interno dello stesso DNS
    - Reperibile in modo efficiente (query DNS)
    - La chiave di un dominio può essere firmata solo dalla chiave del dominio di livello superiore (parent domain).

      Sicuro: unico "trusted path" dalla root al dominio