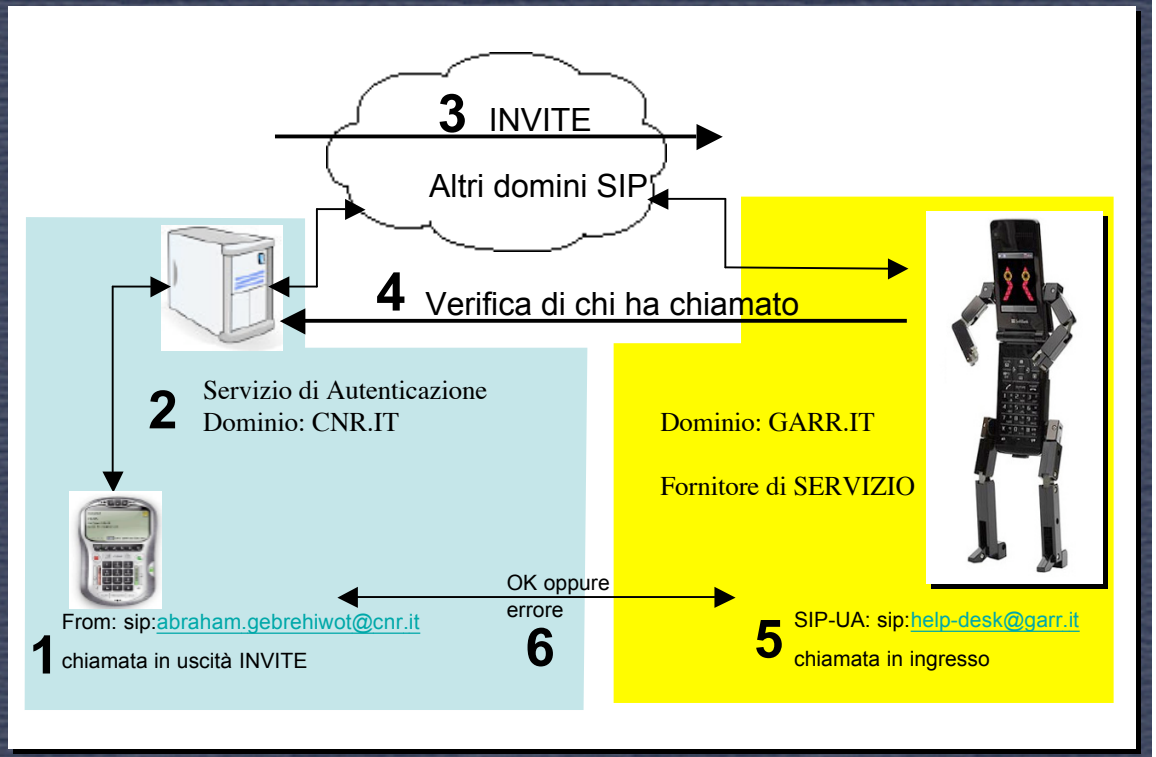
Abraham Gebrehiwot
CNR Istituto di Informatica e Telematica - Pisa

Attività di TERENA sulla SIP identity

Problema da risolvere: Si vuole accertare l'identità del chiamante

- integrità e autenticità dei messaggi SIP
- Identificazione del chiamante
  - Chi è il chiamante?
  - Da dove chiama?
  - Cosa fa?
  - Dove lavora?
  - Ha credito?
  - ...
- la confidenzialità dei messaggi SIP non è un aspetto trattato in questa presentazione
- La sicurezza di messaggi SIP ha nulla a che fare con "media encription"

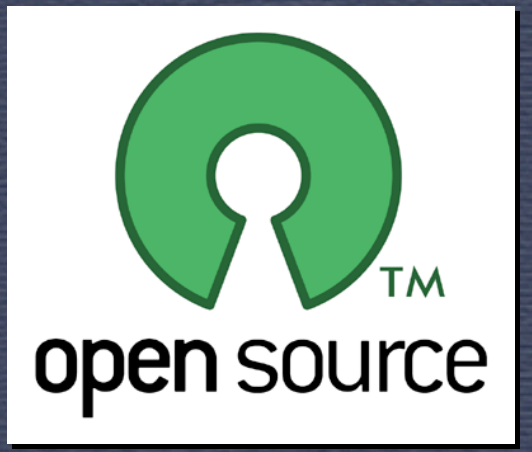


Introduzione

- RFC 3261 - SIP: Session Initiation Protocol
  - Identificazione del chiamante a livello Intra-Domain
- RFC 4474 - Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)
  - Certificazione dell'autenticità dei campi del messaggio SIP a livello Inter-Domain
- RFC 4484 - Trait-Based Authorization Requirements for the Session Initiation Protocol (SIP)
  - Necessità di identificazione del chiamante e del suo ruolo a livello Inter-Domain
- SIP SAML Profile and Binding (draft-ietf-sip-saml-03.txt scade il 21 maggio 2008)
  - Implementazione di meccanismi di autorizzazione federata basati su SAML 2
  - Obbiettivo di soddisfare i requisiti presentati in RFC 4484

Introduzione

- Implementazioni e progetti Open Source
  - SER
    - supporto di TLS
    - Supporto di RFC 4474
  - OpenSER
    - supporto di TLS
    - Roadmap RFC 4474
      - patch non ufficiale e non completamente funzionante
  - Asterisk
    - molto indietro su aspetti simili
    - la versione 1.6 supporta TLS (versione beta)



Meccanismi standard descritti in RFC-3261

- RFC 3261 - SIP: Session Initiation Protocol
  - Soluzioni:
    - Autenticazione digest
    - Transport Layer Security
    - S/MIME
  - Inconvenienti:
    - soluzioni non scalabili
  - Supportato in tutto/in parte da prodotti Open Source
    - SER, OpenSER, Asterisk e molti SIP-UA

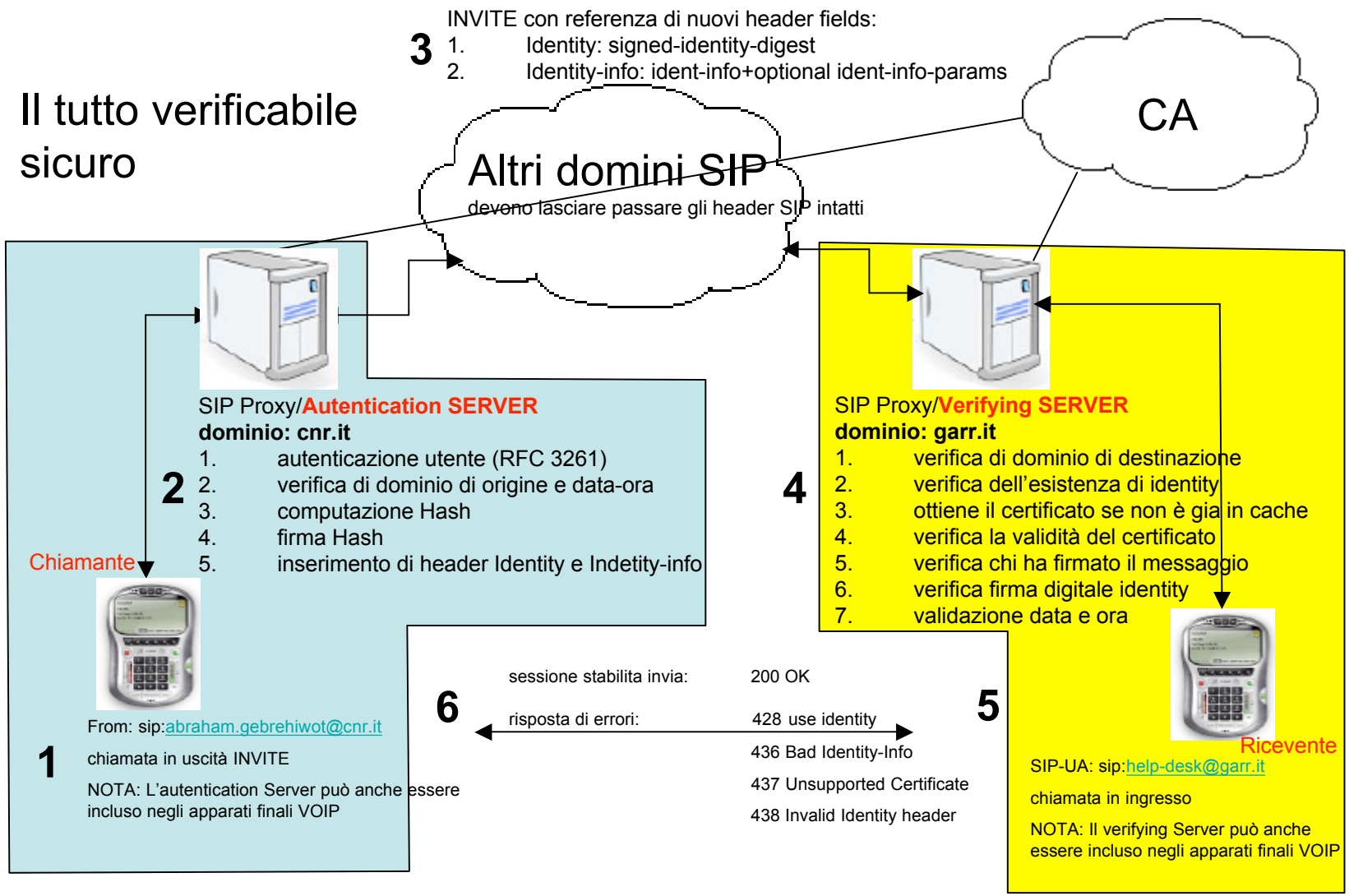
RFC 4474

Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)

- Obiettivo:
  - Estendere l'autenticazione del primo hop a livello inter-domain
  - Certificazione dell'autenticità e integrità dei campi del messaggio SIP a livello Inter-Domain
- Definizione di nuovi SIP header fields
  - Identity
  - Identity-Info
- Nessuna precedente associazione con l'identità del chiamante
- Architettura di autenticazione mediata: due nuovi servizi
  - Servizio di "autenticazione" e "verifica"
    - Normalmente tali funzioni sono implementate dai SIP proxy
      - Potrebbero essere implementate sui SIP-UA garantendo sicurezza end-to-end
    - Non dipendono da altri funzionalità SIP
      - Questo lo rende ancora più attraente

RFC 4474

Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)



INVITE con Identity


```
INVITE sip:bob@biloxi.example.org SIP/2.0
  Via: SIP/2.0/TLS pc33.atlanta.example.com;branch=z9hG4bKnashds8
  To: Bob <sip:bob@biloxi.example.org>
  From: Alice <sip:alice@atlanta.example.com>;tag=1928301774
  Call-ID: a84b4c76e66710
  CSeq: 314159 INVITE
  Max-Forwards: 70
  Date: Thu, 21 Feb 2002 13:02:03 GMT
  Contact: <sip:alice@pc33.atlanta.example.com>
  Identity:
    "ZYNBbHC00VMZr2kZt6VmCvPonWJMGvQTBDqghoWeLxJfzB2a1pxAr3VgrB0SsSAa
     ifsRdiOPoQZYOy2wrVghuhcsMbHWUSFxI6p6q5TOQXHMmz6uEo3svJsSH49thyGn
     FVcnyaZ++yRlBYYQTLqWzJ+KVhPKbfU/pryhVn9Yc6U="
  Identity-Info: <https://atlanta.example.com/atlanta.cer>;alg=rsa-sha1
  Content-Type: application/sdp
  Content-Length: 147

  v=0
  o=UserA 2890844526 2890844526 IN IP4 pc33.atlanta.example.com
  s=Session SDP
  c=IN IP4 pc33.atlanta.example.com
  t=0 0
  m=audio 49172 RTP/AVP 0
  a=rtpmap:0 PCMU/8000
```

digest-string = addr-spec "|" addr-spec "|" callid "|" 1*DIGIT SP Method "|" SIP-date "|" [addr-spec] "|" message-body
Identity = signed-identity-digest

Identity-Info =: ident-Info + optional ident-info-params
ident-info =: absoluteURI

Implementazione di “Authenticated Identity Management” usando il SIP Express Router

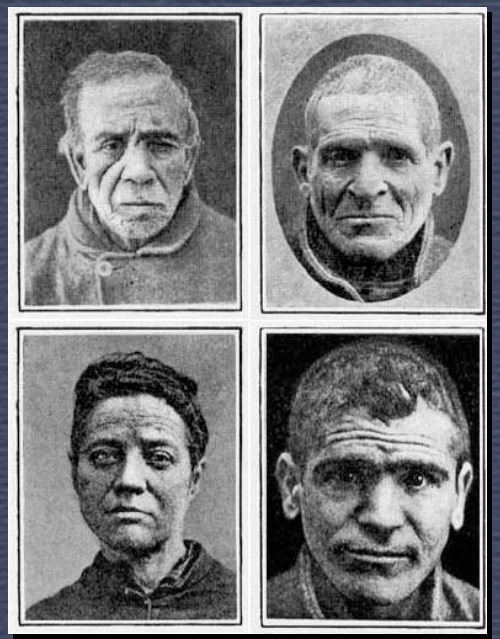
- Implementazione:
  - SER 2.1.x (versione non stabile) distribuzione CVS http://www.iptel.org/download
    - Metodi INVITE, BYE, OPTION e ACK sono firmati
      - Metodi CANCEL e REGISTER non sono supportati
    - Gestione di piu’ realm sullo stesso proxy SIP non supportato
      - estensione subjectAltName dei certificati non supportati
    - Questo modulo non dipende da altri moduli
  - OpenSSL per eseguire funzioni crittografiche
  - Web server possibilmente con supporto SSL (https) per distribuire certificati
  - Certification Authority per rilascio e verifica dei certificati dei server proxy SIP
  - sistema operativo LINUX

- Documento di guida per l’installazione:
  - “Deployment of auth_identity module with SIP Express Router”
    - http://reti4.iit.cnr.it/voiprepository/ser-identity.pdf
      - Riferimento scritto in ambito di un tirocinio presso l’IIT-CNR da due studenti del CLS della facoltà di Ingegneria Informatica
        - Stefano Abbate: stef.abbate@gmail.com
        - Mariantonietta Noemi La Polla: noemi.lapolla@gmail.com

RFC 4484

Trait-Based Authorization Requirements for the Session Initiation Protocol (SIP)

- RFC informativo
- Obiettivo
  - Estendere la prova d'identità di registrazione a livello inter-domain
  - Fornire un framework di autorizzazione più ricco non solo basato sull'identità del chiamante ma sul tratto del chiamante in base ad un "affermazione" del "servizio di autorizzazione"
    - Meccanismi di autenticazioni sono ortogonali a quelli di autorizzazione
    - Molte volte più che l'identità della persona servono i ruoli della persona per permettere l'autorizzazione ad un servizio
    - Migliorare la privacy e anonimato degli utenti
    - L'identità diventa uno degli attributi che può essere divulgato



RFC 4484

Trait-Based Authorization Requirements for the Session Initiation Protocol (SIP)

3 INVITE con referenza di ASSERTION (nuovi SIP header fields)

Prova d'identità con tratto

Altri domini SIP

Trust relationship (federazione)

SIP Proxy SERVER Assertion granting entity
dominio: cnr.it

2
1. autenticazione utente (RFC 3261)
2. Autenticazione e affermazione (con timeout)
   - generando una sorta di token per referenziare l'affermazione generata

SIP Proxy SERVER/Assertion verifying entity
dominio: garr.it

4
1. Richiesta di servizio + referenza di affermazione
2. risposta/Errore

OK oppure

6 messaggi d'errore da definire

5
SIP-UA: sip:help-desk@garr.it

chiamata in ingresso

NOTA: L'assertion verifying entity può anche essere incluso negli apparati finali VOIP

1
From: sip:abraham.gebrehiwot@cnr.it

chiamata in uscità INVITE

NOTA: L'assertion granting entity può anche essere incluso negli apparati finali VOIP

RFC 4484

Trait-Based Authorization Requirements for the Session Initiation Protocol (SIP)

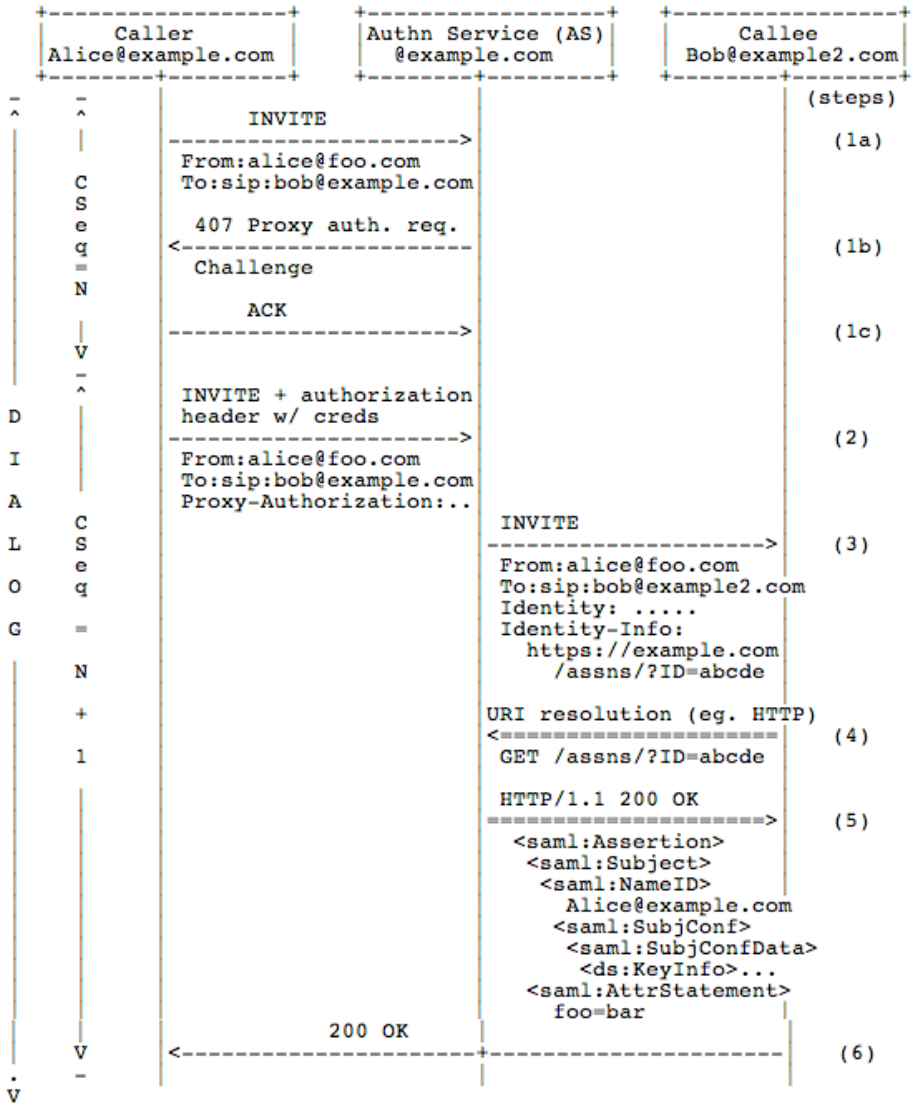
- Meccanismi di fiducia: federazione
  - Una federazione è definita come un insieme di domini amministrativi che attuano politiche comuni per quanto riguarda l'uso e la applicabilità di tratti per le decisioni di autorizzazione
  - Federazione necessariamente implica un rapporto di fiducia (una chiave pre-condivisa o garanzie crittografiche) che una particolare affermazione è stata generata da un servizio di autorizzazione partecipante alla federazione
  - L'asserzione è una sorta di documento costituito da una serie di attributi con garanzie crittografiche fornite dalla parte che l'ha generata (normalmente il gestore del servizio di autorizzazione)

SIP SAML Profile and Binding (DRAFT)

- Obiettivo
  - Soddisfa i requisiti presentati in RFC 4484 - “Trait-Based Authorization Requirements for the Session Initiation Protocol (SIP)”
- SAML2
  - Definisce un framework, basato su XML, per lo scambio di "affermazioni di sicurezza" tra entità
- Draft-ietf-sip-saml-03.txt
  - Scade il 21 maggio 2008
  - Specifica il SIP profile e binding di SAML
  - Meccanismi di autorizzazione federata basati su SAML 2

- Oltre SAML esistono vari modi per risolvere trait-based autorizzazione
  - Authorization certificates [RFC3281],
  - SPKI [RFC2693],
  - Extensions to the authenticated identity body [RFC3893].

SIP-SAML-based Network Asserted Identity



TERENA: tf-ecs

- Si propone di mantenere un sito WEB su cui fare chiarezza su questi aspetti
- Lista di discussione su vari argomenti legati al VOIP
- CD con GnuGK, OpenSER e Asterisk

Attività di TERENA sulla SIP identity

Abraham Gebrehiwot

Telefono cellulare: (+39) 348/7981036
Telefono ufficio (PSTN/ENUM nrenum.net): (+39) 050/3152079
sip:Abraham.Gebrehiwot@iit.cnr.it
e-mail:Abraham.Gebrehiwot@iit.cnr.it
CNR Istituto di Informatica e Telematica - Pisa