Cryptography and Network Security Chapter 15

Fifth Edition

by William Stallings

Lecture slides by Lawrie Brown

Chapter 15 – User Authentication

We cannot enter into alliance with neighboring princes until we are acquainted with their designs.

—*The Art of War*, Sun Tzu

Πιστοποιηση Αυθεντικοτητας Χρηστη (User Authentication)

- Είναι ένα θεμελιωδες δομικο στοιχειο της ασφαλειας
  - Είναι η βαση του ελεγχου προσβασης χρηστη και της αποδοσης ευθυνων (accountability) στους χρηστες
- Είναι η διαδικασια επιβεβαιωσης μιας ιδιοτητας που ισχυριζεται ότι εχει μια οντοτητα του συστηματος
- Εχει δυο βηματα:
  - Προσδιορισμος (identification)
  - Επιβεβαιωση (verification)
- Είναι κατι διαφορετικο από την πιστοποιηση αυθεντικοτητας μηνυματος

Μεσα Πιστοποιησης Αυθεντικοτητας Χρηστη (Means of User Authentication)

- Υπαρχουν 4 μεσα για την πιστοποιηση της αυθεντικοτητας χρηστη
- Να βασιστουμε σε κατι το μοναδικο
  - Που γνωριζει - π.χ. password, PIN
  - Που κατεχει – π.χ. key, token, smartcard
  - Που ειναι (στατικα βιομετρικα) – π.χ. δακτυλικα αποτυπωμα, ιριδα
  - Που κανει (δυναμικα βιομετρικα) - π.χ. φωνη
- Καθενα από τα παραπανω, μπορει να χρησιμοποιηθει μονο ή σε συνδυασμό με αλλο
- Ολα μπορουν να παρεχουνε πιστοποιηση αυθεντικοτητας χρηστη

Πρωτοκολλα Πιστοποιησης Αυθεντικοτητας (Authentication Protocols)

- Χρησιμοποιουνται για να πεισουν το κάθε μερος για την ταυτοτητα του αλλου και για την ανταλλαγη κλειδιων συνοδου
- Μπορει να είναι μονοδρομη ή αμοιβαια
- Σημαντικα σημεια είναι:
  - Εμπιστευτικοτητα – για την προστασια των κλειδιων συνοδου
  - Το χρονικο πλαισιο – για την αποφυγη επιθεσεων επαναληψης

Επιθεσεις Επαναληψης

- Οπου ένα νομιμο και υπογεγραμμενο μηνυμα αντιγραφεται και αργοτερα ξαναστελνεται
  - Απλη επαναληψη
  - Επαναληψη που μπορει να καταγραφει
  - Επαναληψη που δεν μπορει να ανιχνευτει
  - Προς τα πισω επαναληψη χωρις τροποποιηση
- Τα μεσα αποφυγης της περιλαμβανουν
  - Τη χρηση ακολουθιακων αριθμων (αυτό είναι γενικα μη πρακτικο)
  - Χρονοσφραγιδες (απαιτουν συγχρονισμενα ρολογια)
  - Προκληση/αποκριση (χρησιμοποιωντας μοναδικη nonce)

Μονοδρομη Πιστοποιηση Αυθεντικοτητας

- Απαιτειται όταν ο αποστολεας και ο παραληπτης δεν βρισκονται σε επικοινωνια την ιδια ωρα (π.χ. email)
- Ο header είναι μη κρυπτογραφημενος και μπορει να παραληφθει απο το email system
- Μπορει όμως να θελουμε τα περιεχομενα να είναι κρυπτογραφημενα και να πιστοποιειται η αυθεντικοτητα του αποστολεα.

Χρηση Συμμετρικης Κρυπτογραφησης

- Οπως συζητησαμε και σε προηγουμενο μαθημα μπορουμε να χρησιμοποιησουμε ιεραρχια δυο επιπεδων κλειδιων
- Συνηθως με ένα εμπιστο κεντρο διανομης κλειδιου (KDC)
  - Κάθε πλευρα μοιραζεται ένα δικο της master key με το KDC
  - Το KDC δημιουργει κλειδια συνοδου για συνδεσεις μεταξυ των μερων
  - Τα master keys χρησιμοποιουνται για τη διανομη των κλειδιων συνοδου

Πρωτοκολλο Needham-Schroeder

- Είναι ένα αυθεντικο πρωτοκολλο διανομης κλειδιου με τριτη εμπιστη οντοτητα
- Για συνοδο μεταξυ των A και B με τη διαμεσολαβηση του KDC
- Η επισκοπιση του πρωτοκολλου ειναι:
  1. A->KDC: $ID_A \,||\, ID_B \,||\, N_1$
  2. KDC -> A: $E(K_a,[K_s||ID_B||N_1||\, E(K_b,[K_s||ID_A])])$
  3. A -> B: $E(K_b, [K_s||ID_A])$
  4. B -> A: $E(K_s, [N_2])$
  5. A -> B: $E(K_s, [f(N_2)])$

Πρωτοκολλο Needham-Schroeder

- Χρησιμοποιειται για να διανεμηθει ένα νέο κλειδι συνοδου για επικοινωνιες μεταξυ του Α και του Β
- Αλλα είναι τρωτο σε επιθεσεις επαναληψης αν μια παλιοτερη συνοδος εχεις υποκλαπει.
  - Τοτε το μηνυμα 3 μπορει να ξανασταλει πειθοντας τον Β ότι επικοινωνει με τον Α
- Τροποποιησεις για να αντιμετωπιστει αυτό το προβλημα απαιτουν:
  - Χρονοσφραγιδες στα βηματα 2 & 3 (Denning 81)
  - Χρηση μιας επιπλεον nonce (Neuman 93)

Μονοδρομη Πιστοποιηση Αυθεντικοτητας (One-Way Authentication)

- Χρησιμοποιουμε τροποποιηση του KDC για ασφαλες email
  - Επειδη ο Β δεν είναι online, παραλειπονται τα βηματα 4 & 5
- Το πρωτοκολλο που προκυπτει γινεται:

  1. A->KDC: $ID_A \,||\, ID_B \,||\, N_1$

  2. KDC -> A: $E(K_a, [K_s||ID_B||N_1 \,||\, E(K_b,[K_s||ID_A])])$

  3. A -> B: $E(K_b, [K_s||ID_A]) \,||\, E(K_s, M)$
- Παρεχει κρυπτογραφηση και καποια πιστοποιηση αυθεντικοτητας
- Δεν παρεχει προστασια από επιθεση επαναληψης

Kerberos

- Συστημα εμπιστου εξυπηρετη κλειδιου που αναπτυχθηκε στο MIT.
- Παρεχει ένα κεντρικο συστημα πιστοποιησης αυθεντικοτητας, με τριτη εμπιστη οντοτητα και συμμετρικη κρυπτογραφια
  - Επιτρεπει στους χρηστες να προσπελαυνουν τις κατανεμημενες υπηρεσιες μεσω δικτυου
  - Χωρις να χρειαζεται να εμπιστευονται ολους τους τους workstations
  - Αρκει να εμπιστευονται έναν κεντρικο authentication server
- Χρησιμοποιουνται δυο εκδοσεις του Κερβερου: 4 & 5

Απαιτησεις του Κερβερου

- Η πρωτη αναφορα προσδιορισε τις απαιτησεις ως εξης:
  - Ασφαλης (secure)
  - Αξιοπιστος (reliable)
  - Διαφανης (transparent)
  - Επεκτασιμος (scalable)
- Υλοποιειται χρησιμοποιωντας ένα πρωτοκολλο πιστοποιησης αυθεντικοτητας βασισμενο στο πρωτοκολλο Needham-Schroeder

Επισκοπιση του Kerberos v4

- Είναι ενα βασικο σχημα πιστοποιησης αυθεντικοτητας με χρηση τριτης εμπιστης οντοτητας (third-party)
- Εχει έναν Authentication Server (AS)
  - Οι χρηστες αρχικα διαπραγματευονται με τον AS για να προσδιορισουν τον εαυτο τους
  - Ο AS παρεχει ένα μη φθαρτό αποδεικτικό ταυτότητας (non-corruptible authentication credential) που ονομαζεται ticket granting ticket (TGT).
- Υπαρχει ενας Ticket Granting server (TGS)
  - Οι χρηστες στη συνεχεια ζητουν προσβαση σε άλλες υπηρεσιες από τον TGS με βαση τα TGT
- Εφαρμοζεται ένα συνθετο πρωτοκολλο που χρησιμοποιει τον DES

Διαλογος του Kerberos v4

(1) C → AS $ID_c \| ID_{tgs} \| TS_1$

(2) AS → C $E(K_c, [K_{c,tgs} \| ID_{tgs} \| TS_2 \| Lifetime_2 \| Ticket_{tgs}])$

$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \| ID_C \| AD_C \| ID_{tgs} \| TS_2 \| Lifetime_2])$

(a) Authentication Service Exchange to obtain ticket-granting ticket

(3) C → TGS $ID_v \| Ticket_{tgs} \| Authenticator_c$

(4) TGS → C $E(K_{c,tgs}, [K_{c,v} \| ID_v \| TS_4 \| Ticket_v])$

$Ticket_{tgs} = E(K_{tgs}, [K_{c,tgs} \| ID_C \| AD_C \| ID_{tgs} \| TS_2 \| Lifetime_2])$

$Ticket_v = E(K_v, [K_{c,v} \| ID_C \| AD_C \| ID_v \| TS_4 \| Lifetime_4])$

$Authenticator_c = E(K_{c,tgs}, [ID_C \| AD_C \| TS_3])$

(b) Ticket-Granting Service Exchange to obtain service-granting ticket

(5) C → V $Ticket_v \| Authenticator_c$

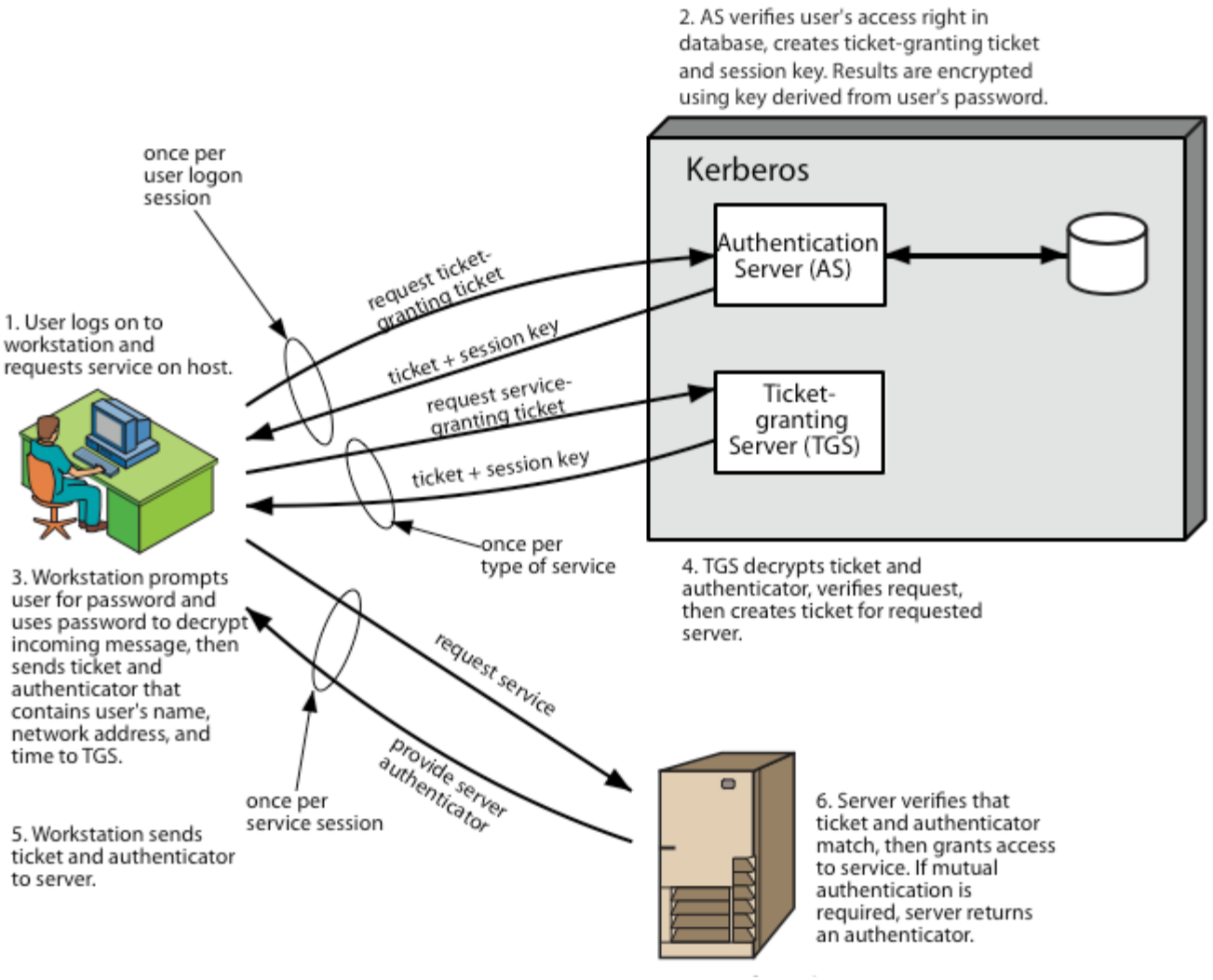
(6) V → C $E(K_{c,v}, [TS_5 + 1])$ (for mutual authentication)

$Ticket_v = E(K_v, [K_{c,v} \| ID_C \| AD_C \| ID_v \| TS_4 \| Lifetime_4])$

$Authenticator_c = E(K_{c,v}, [ID_C \| AD_C \| TS_5])$

(c) Client/Server Authentication Exchange to obtain service

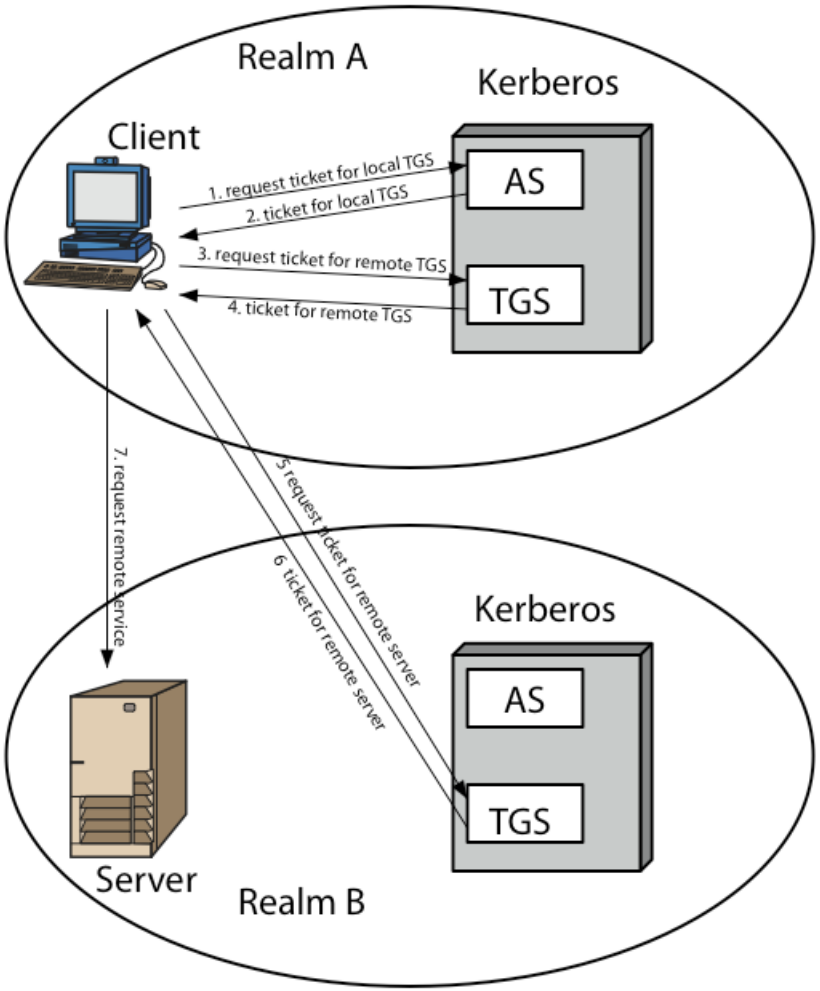
Επισκοπιση του Kerberos 4



Kerberos Realms

- Ένα περιβαλλον Kerberos αποτελειται απο:
  - Εναν Kerberos server
  - Εναν αριθμο από clients, που ολοι εχουν εγγραφει στον server
  - Application servers, που μοιραζονται κλειδια με τον server
- Αυτο αποκαλειται «realm»
  - Συνηθως είναι ένα ενιαιο διαχειριστικο πεδιο (administrative domain)
- Αν εχουμε πολλαπλα realms, οι εξυπηρετες Kerberos αυτων πρεπει να μοιραζονται κλειδια και να εμπιστευονται ο ενας τον αλλον

Kerberos Realms



Kerberos Version 5

- Αναπτυχθηκε στα μεσα της δεκαετιας του 1990.
- Προσδιοριστηκε ως Internet standard RFC 1510
- Παρεχει βελτιωσεις σε σχεση με την εκδοση 4.
  - Αντιμετωπιζει περιορισμους του περιβαλλοντος
    - encryption algorithm, network protocol, byte order, ticket lifetime, authentication forwarding, interrealm authentication
  - Και τεχνικες ελλειψεις
    - double encryption, non-std mode of use, session keys, password attacks

Kerberos v5 Dialogue

(1) C → AS Options ‖ ID_c ‖ $Realm_c$ ‖ ID_{tgs} ‖ $Times$ ‖ $Nonce_1$

(2) AS → C $Realm_c$ ‖ ID_C ‖ $Ticket_{tgs}$ ‖ $E(K_c, [K_{c,tgs} \| Times \| Nonce_1 \| Realm_{tgs} \| ID_{tgs}])$

$Ticket_{tgs} = E(K_{tgs}, [Flags \| K_{c,tgs} \| Realm_c \| ID_C \| AD_C \| Times])$

(a) Authentication Service Exchange to obtain ticket-granting ticket

(3) C → TGS Options ‖ ID_v ‖ $Times$ ‖ ‖ $Nonce_2$ ‖ $Ticket_{tgs}$ ‖ $Authenticator_c$

(4) TGS → C $Realm_c$ ‖ ID_C ‖ $Ticket_v$ ‖ $E(K_{c,tgs}, [K_{c,v} \| Times \| Nonce_2 \| Realm_v \| ID_v])$

$Ticket_{tgs} = E(K_{tgs}, [Flags \| K_{c,tgs} \| Realm_c \| ID_C \| AD_C \| Times])$

$Ticket_v = E(K_v, [Flags \| K_{c,v} \| Realm_c \| ID_C \| AD_C \| Times])$

$Authenticator_c = E(K_{c,tgs}, [ID_C \| Realm_c \| TS_1])$

(b) Ticket-Granting Service Exchange to obtain service-granting ticket

(5) C → V Options ‖ $Ticket_v$ ‖ $Authenticator_c$

(6) V → C $E_{K_{C,V}}$ [TS_2 ‖ Subkey ‖ Seq#]

$Ticket_v = E(K_v, [Flags \| K_{c,v} \| Realm_c \| ID_C \| AD_C \| Times])$

$Authenticator_c = E(K_{c,v}, [ID_C \| Realm_c \| TS_2 \| Subkey \| Seq\#])$

(c) Client/Server Authentication Exchange to obtain service

Πιστοποιηση Αυθεντικοτητας Μακρυνου Χρηστη

- Σε προηγουμενο μαθημα ειδαμε τη χρηση ενος κρυπτογραφιας δημοσιου κλειδιου για διανομη κλειδιου συνοδου
  - Υποθετουμε ότι και τα δυο μερη εχουν ο ενας το δημοσιο κλειδι του αλλου
  - Αυτό ισως δεν είναι και τοσο πρακτικο
- Εχουμε το πρωτοκολλο Denning που χρησιμοποιει χρονοσφραγιδες (timestamps)
  - Χρησιμοποιει εναν κεντρικο authentication server (AS) για να παρεχει πιστοποιητικα δημοσιου κλειδιου
  - Απαιτει συγχρονισμενα ρολογια
- Επισης εχουμε και το πρωτοκολλο Woo & Lam που χρησιμοποιει nonces

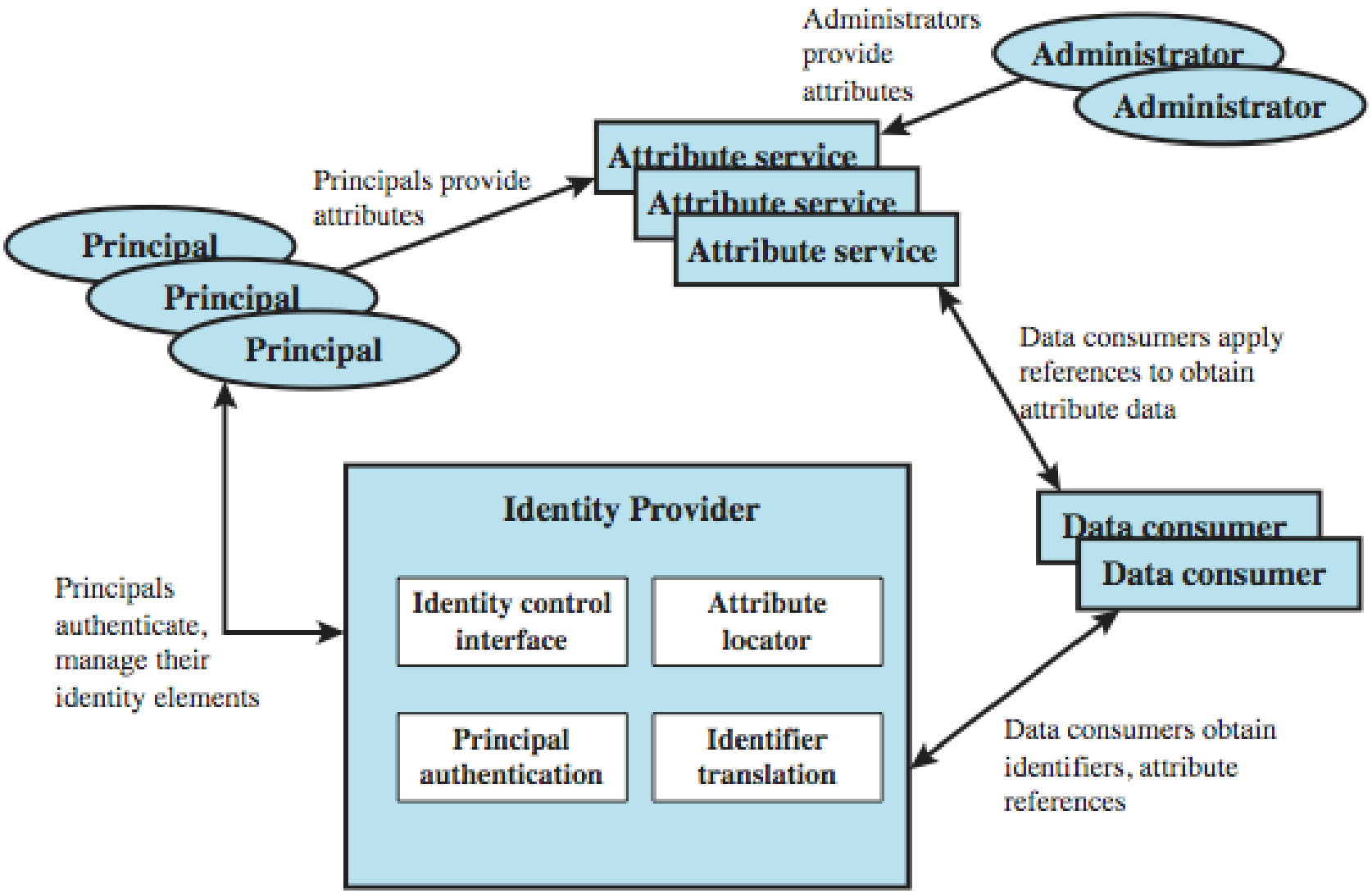
Μονοδρομη πιστοποιηση αυθεντικοτητας

- Υπαρχουν προσεγγισεις δημοσιου κλειδιου για το email
  - Κρυπτογραφηση μηνυματος για εμπιστευτικοτητα, πιστοποιηση αυθεντικοτητας ή και τα δυο
  - Πρεπει να είναι γνωστα τα δημοσια κλειδια
  - Χρησιμοποιουνται δαπανηροι αλγοριθμοι δημοσιου κλειδιου σε μεγαλα μηνυματα
- Για εμπιστευτικοτητα κρυπτογραφησε το μηνυμα με ένα μυστικο κλειδι μιας χρησης που κρυπτογραφειται με αλγοριθμο δημοσιου κλειδιου
- Για πιστοποιηση αυθεντικοτητας του μηνυματος χρησιμοποιησε ψηφιακη υπογραφη
- Χρησιμοποιησε ψηφιακο πιστοποιητικο για την παροχη δημοσιου κλειδιου

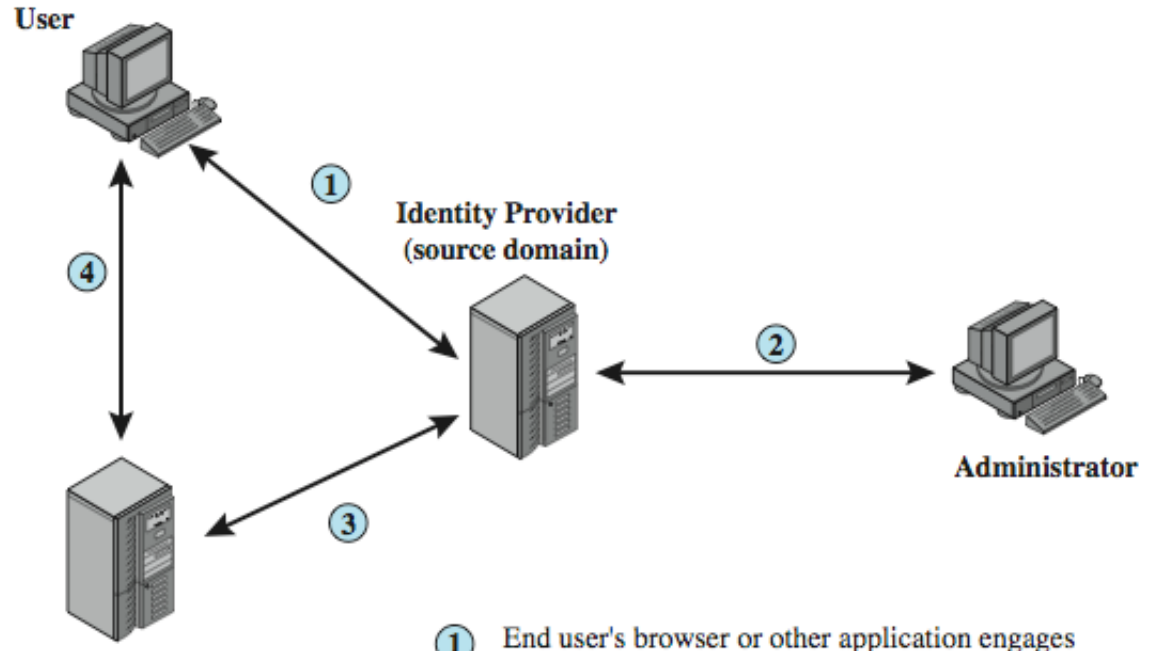
Federated Identity Management

- Χρησιμοποιειται ένα κοινο σχημα διαχειρισης ταυτοτητας
  - Κατα μηκος πολλαπλων enterprises & πολλων εφαρμογων
  - Υποστηριζονται πολλες χιλιαδες ή και εκατομμυρια χρηστες
- Τα βασικα στοιχεια ειναι:
  - authentication, authorization, accounting, provisioning, workflow automation, delegated administration, password synchronization, self-service password reset, federation
- Ο Kerberos περιεχει πολλα απο αυτα τα στοιχεια

Identity Management



Identity Federation



1. End user's browser or other application engages in an authentication dialogue with identity provider in the same domain. End user also provides attribute values associated with user's identiy.

2. Some attributes associated with an identity, such as allowable roles, may be provided by an administrator in the same domain.

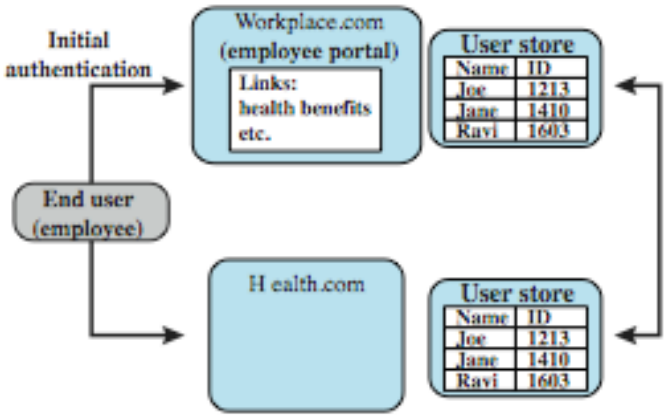
3. A service provider in a remote domain, which the user wishes to access, obtains identity information, authentication information, and associated attributes from the identity provider in the source domain.

4. Service provider opens session with remote user and enforces access control restrictions based on user's identity and attributes.

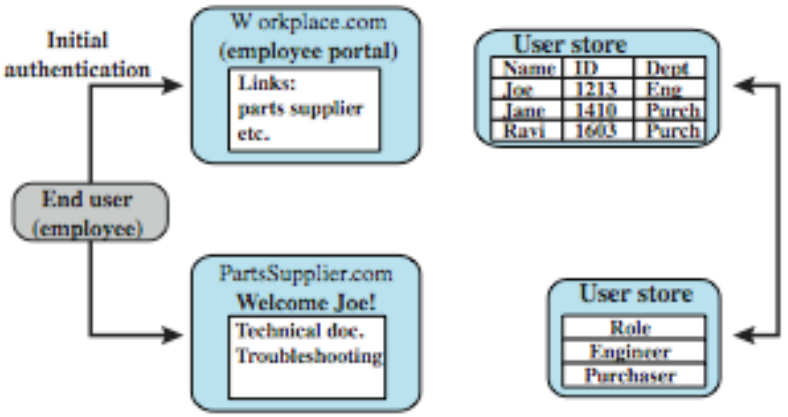
Χρησιμοποιουμενα Standards

- Security Assertion Markup Language (SAML)
  - Είναι μια γλωσσα βασισμενη στην XML, για ανταλλαγη πληροφοριας μεταξυ business partners
- Είναι μερος του προτυπου OASIS (Organization for the Advancement of Structured Information Standards) για federated identity management
  - π.χ. WS-Federation για browser-based federation
- Χρειαζονται καποια ωριμα βιομηχανικα προτυπα

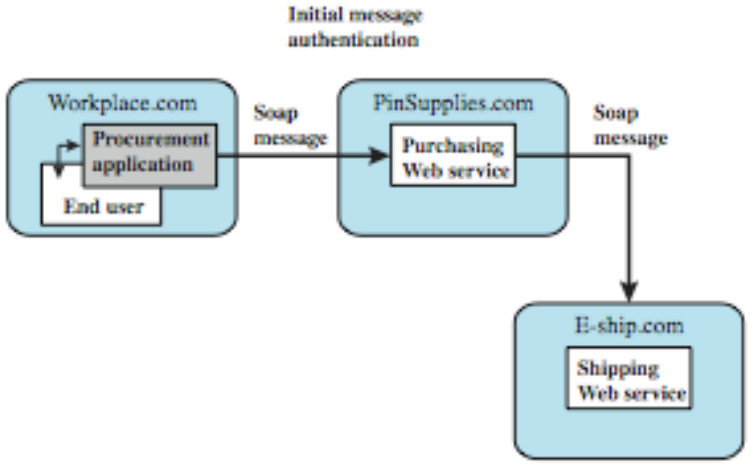
Federated Identity Examples



(a) Federation based on account linking



(b) Federation based on roles



(b) Chained Web Services

Συνοψη

- Εξετασαμε:
  - Θεματα πιστοποιησης αυθεντικοτητας μακρυνου χρηστη (remote user authentication)
  - Πιστοποιηση αυθεντικοτητας με χρηση συμμετρικης κρυπτογραφιας (symmetric encryption)
  - Το συστημα Kerberos
  - Την Πιστοποιηση αυθεντικοτητας με χρηση ασυμμετρης κρυπτογραφιας
  - federated identity management