Single Sign On & Software Libero


Michele Baldessari


<michele@pupazzo.org>


michele@jabber.pupazzo.org


E4B4 4826 0E0C BF0D 3935 ED35 A1F6 EE94 *240B 4C3D*

Single Sign On & Software Libero

- Introduzione
- Single Sign On
- Kerberos
- Installazione / Configurazione
- Integrazione con altri S.O.
- Futuri sviluppi

Single Sign On & Software Libero

- **Introduzione**
- Identity Management
- AAA
- Crittografia

Single Sign On & Software Libero

- **Identity Management**
- Fondamentalmente indica un insieme di tecnologie volte alla gestione efficiente delle identità in un sistema complesso
- Ha lo scopo di risolvere le difficoltà di gestire un sistema IT complesso con molteplici attori e servizi (dipendenti, clienti, fornitori, partner, consulenti, ispettori)

Single Sign On & Software Libero

- **Identity Management (2)**
- Si occupa inoltre di:
  - *Access Management*
  - *User Management*
  - *Provisioning*
  - *Authentication*
  - *User Data Store (Directory)*
  - *Federated IM*
- IAM – Identity & Access Management

Single Sign On & Software Libero

- **AAA**
- Autenticazione
  - Verifica dell'identità delle parti (persone fisiche o macchine)
- User + Password
- Chiave o certificato
- Chiave o certificato su smart card / token
- Biometria

Single Sign On & Software Libero

- **AAA (2)**
- Autorizzazione
  - Assegnazione dei diritti/permessi all'entità autenticata a seconda delle policy previste
- DAC / MAC
- Permessi
- ACL

Single Sign On & Software Libero

- **AAA (3)**
- Auditing
  - La possibilità di ottenere un *Audit Trail*, una traccia delle azioni (rilevanti) di un utente o di un programma
- Unix Syslog
- Windows Event Log
- Auditing infrastructure

Single Sign On & Software Libero

- **Crittografia**
- Simmetrica
  - La stessa chiave segreta per criptare e decriptare
  - Gestione complessa delle chiavi [*n* entità -> *n * (n – 1) / 2* chiavi, *O(n^2)]*
  - Protocolli: SSL, TLS, Kerberos, IPSEC, ...
  - Algoritmi: AES, ARC4, DES, 3DES, ...

Single Sign On & Software Libero

- **Crittografia**
- Asimmetrica
  - Coppie di chiavi legate matematicamente tra loro, una *pubblica* e una *privata*
  - Gestione lineare delle chiavi [*n* entità -> ~*n* *(coppie di)* chiavi*, O(n)]*
  - Protocolli: SSL, TLS, PGP, S/MIME, IKE, SSH, ...
  - Algoritmi: RSA, DSA, EL GAMAL, DSS

Single Sign On & Software Libero

- **Single Sign On**
- Definizione
- Motivazione
- Protocolli (Kerberos,Web-SSO,SESAME, ...)
- Software proprietario
- Software libero

Single Sign On & Software Libero

- **Definizione**
- **SINGOLA** autenticazione dell'utente
- Successivo accesso a servizi di rete in modo trasparente
- Una unica base di autenticazione (i.e. Servizio di Directory) **non** è di per sè SSO, è la base su cui costruire un'infrastruttura di SSO (è condizione ”praticamente” *necessaria*)

Single Sign On & Software Libero

- **Motivazione**
- Semplificare la vita all'utente
- Singola fonte di autenticazione
- Password policy unica
- Diminuzione costi di Help Desk
- Gestione centralizzata

Single Sign On & Software Libero

- **Protocolli**
- Svariati protocolli di autenticazione che implementano una forma di SSO:
  - Kerberos
  - SESAME
  - CAS
  - OpenID
  - BBAUTH
  - A-Select

Single Sign On & Software Libero

- **Software Proprietario**
- Impossibile adattare applicazioni esistenti per il SSO (*se già non lo supportano*)
- Sono due la possibili strade: quelle con agenti che replicano la informazioni di autenticazione sui vari sistemi e quelle che spesso vengono chiamate *Enterprise Single Sign On* e che lavorano a livello client

Single Sign On & Software Libero

- **Software Proprietario (2)**
- Lato *Client*
- La nomenclatura più adatta sarebbe forse *”Client-side Hacks”*
- Sono programmi che intercettano le login a password degli applicativi legacy
- Memorizzano queste info al primo login
- Inviano in automatico ai login successivi
- Intercettano i cambi password

Single Sign On & Software Libero

- **Software Proprietario (3)**
- L'altro approccio verso il SSO nel mondo proprietario è quello di un datastore centrale e una serie di agent sugli altri sistemi (con meccanismi push/pull)
- Un workflow che definisce le regole di sincronizzazione delle password e/o della gestione degli utenti e gruppi
- Sistema complesso e fragile

Single Sign On & Software Libero

- **Software Libero**
- Possibilità di modificare le applicazioni esistenti per il SSO
- *”Client-side Hacks”* non più necessari
- L'infrastruttura IT può diventare uniforme per quel che riguarda l'autenticazione
- Ancora **molta** strada da fare

Single Sign On & Software Libero

- **Kerberos**
- Introduzione
- Protocollo
- Implementazioni esistenti (MIT, Heimdal, Active Directory)
- Pro / Contro

Single Sign On & Software Libero

- **Introduzione**
- Nasce al MIT dal progetto Athena ('80)
- Prima versione pubblica v4 (1989)
- Protocollo di Single-Sign-On più utilizzato
- Implementato su *NIX, Windows >= 2000, Mac OS X

Single Sign On & Software Libero

- **Introduzione (2)**
- Scritto appositamente per reti ostili
- Single Sign On per qualsiasi tipo di servizio (*modificato appositamente*)
- Autenticazione reciproca e distribuita
- Utilizza crittografia simmetrica
- Needham-Schroeder

Single Sign On & Software Libero

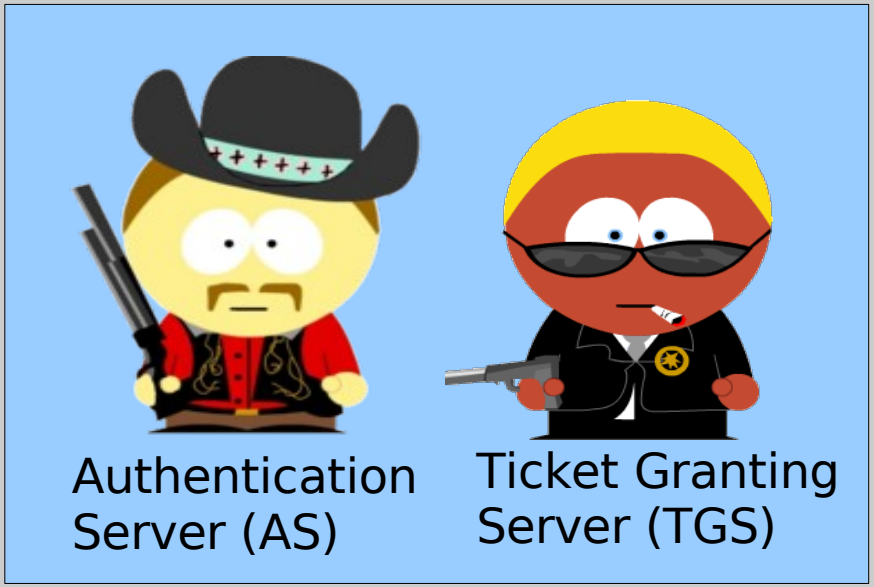
- **Introduzione (3)**
- *Realm* – dominio di autenticazione Kerberos (tipicamente è il dominio DNS in maiuscolo: *LUGBZ.ORG*)
- *Principal* – Ogni entry presente nel database kerberos a cui è associata una chiave segreta
  - *part{/part}@REALM*
  - *michele@LUGBZ.ORG, michele/admin@LUGBZ.ORG*
  - *LDAP/srvldap.lugbz.org@LUGBZ.ORG*

Single Sign On & Software Libero

- **Introduzione (4)**
- *KDC* – Key Distribution center
  - Database di tutti i principal
  - Authentication Server
  - Ticket Granting Server

Single Sign On & Software Libero

Key Distribution Center (KDC)

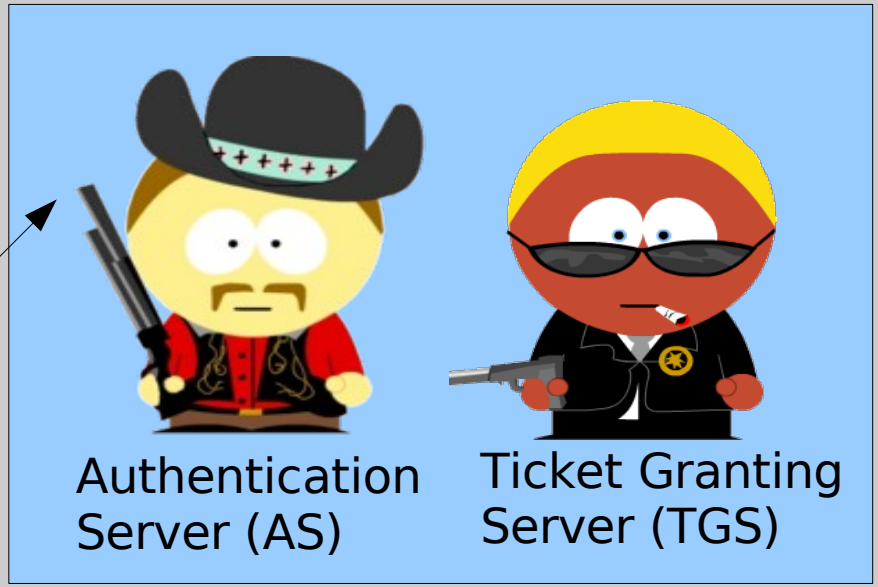


Utente

Networked Service

Single Sign On & Software Libero

Key Distribution Center (KDC)



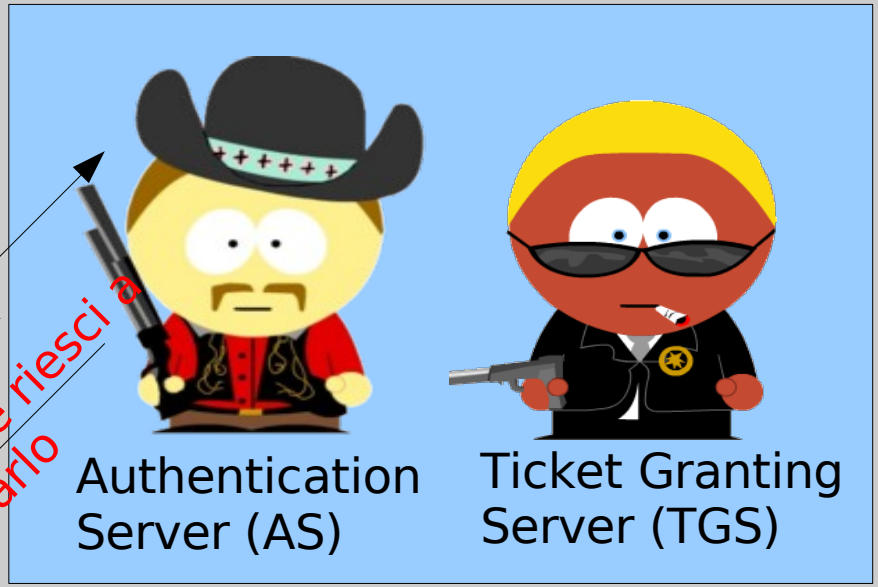
1. Sono Alice, mi serve un TGT

Utente

Networked Service

Single Sign On & Software Libero

Key Distribution Center (KDC)



1. Sono Alice, mi serve un TGT

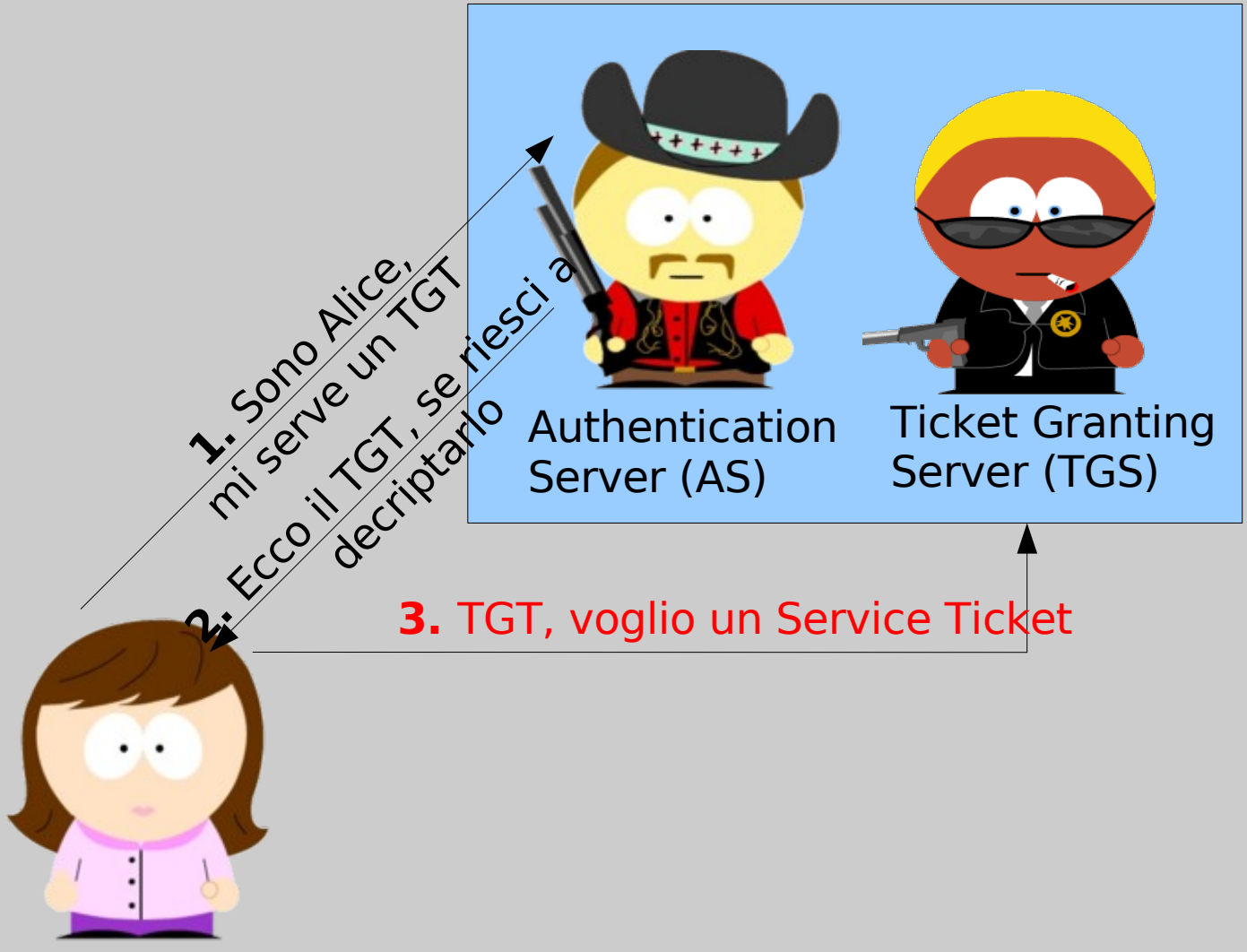
2. Ecco il TGT, se riesci a decriptarlo

Utente

Networked Service

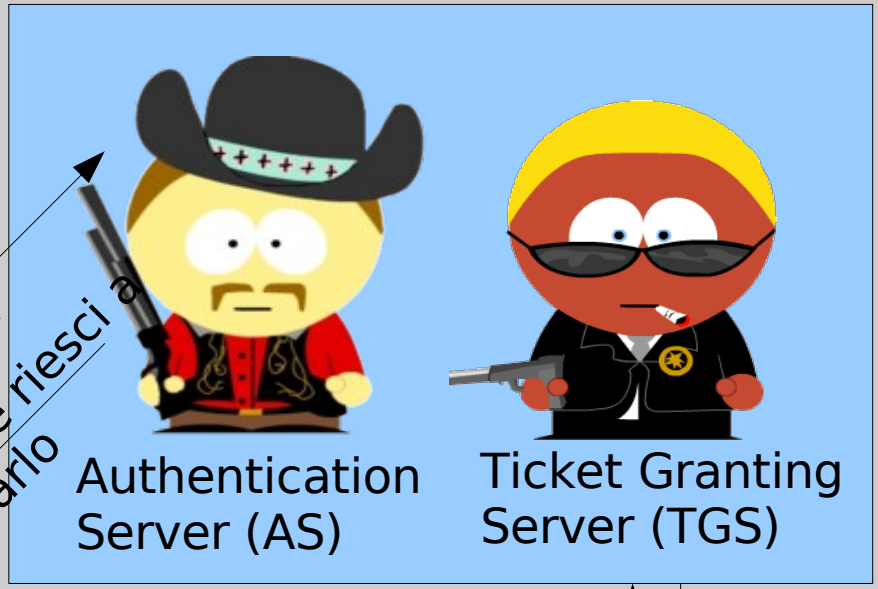
Single Sign On & Software Libero

Key Distribution Center (KDC)



Single Sign On & Software Libero

Key Distribution Center (KDC)

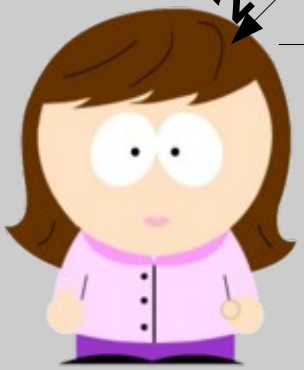


1. Sono Alice, mi serve un TGT

2. Ecco il TGT, se riesci a decriptarlo

3. TGT, voglio un Service Ticket

4. Ecco il Service Ticket

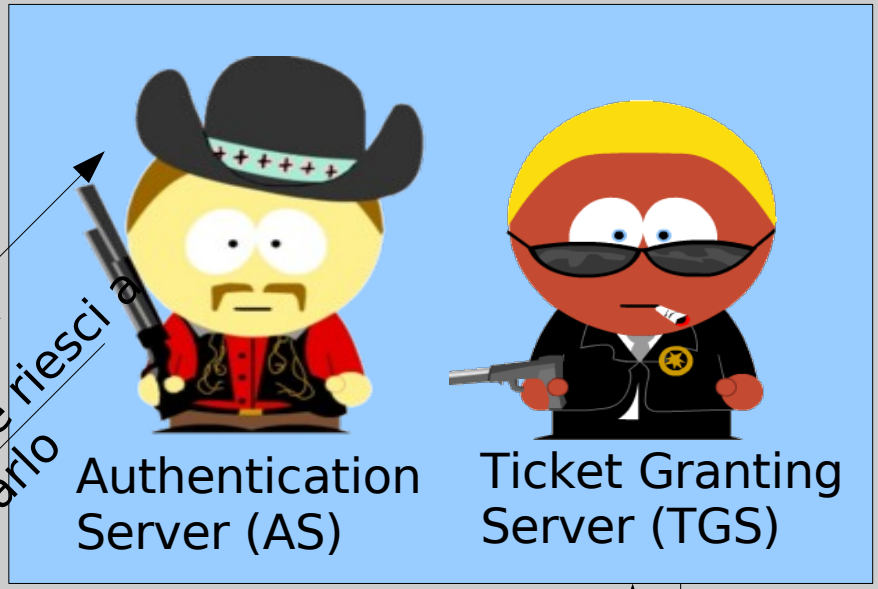


Utente

Networked Service

Single Sign On & Software Libero

Key Distribution Center (KDC)



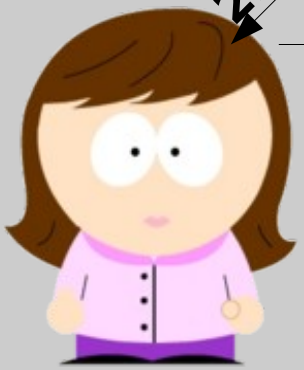
1. Sono Alice, mi serve un TGT

2. Ecco il TGT, se riesci a decriptarlo

3. TGT, voglio un Service Ticket

4. Ecco il Service Ticket

5. Autenticami, ho il Service Ticket

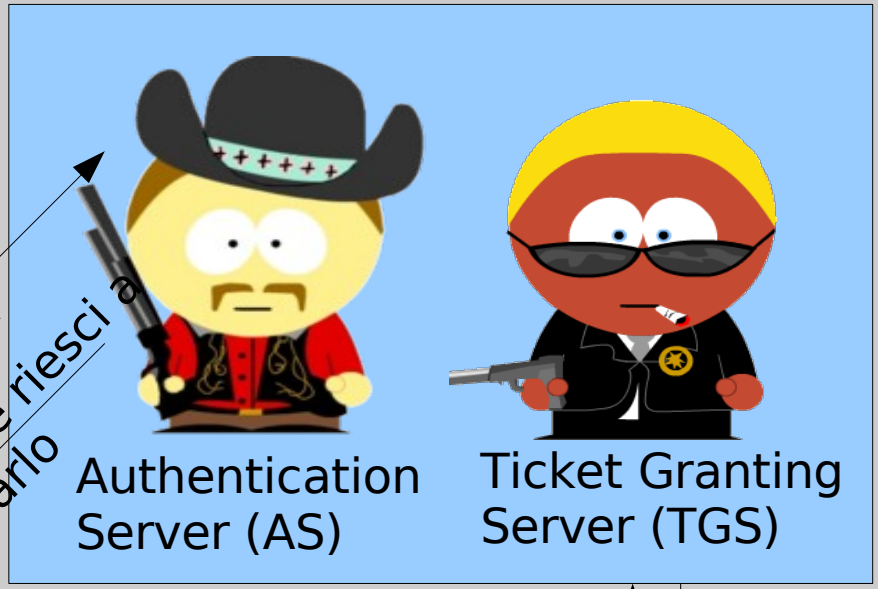


Utente

Networked Service

Single Sign On & Software Libero

Key Distribution Center (KDC)



1. Sono Alice, mi serve un TGT

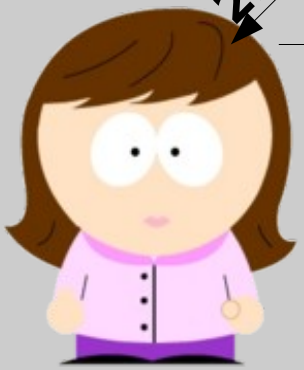
2. Ecco il TGT, se riesci a decriptarlo

3. TGT, voglio un Service Ticket

4. Ecco il Service Ticket

5. Autenticami, ho il Service Ticket

6. Ciao Alice, parliamo

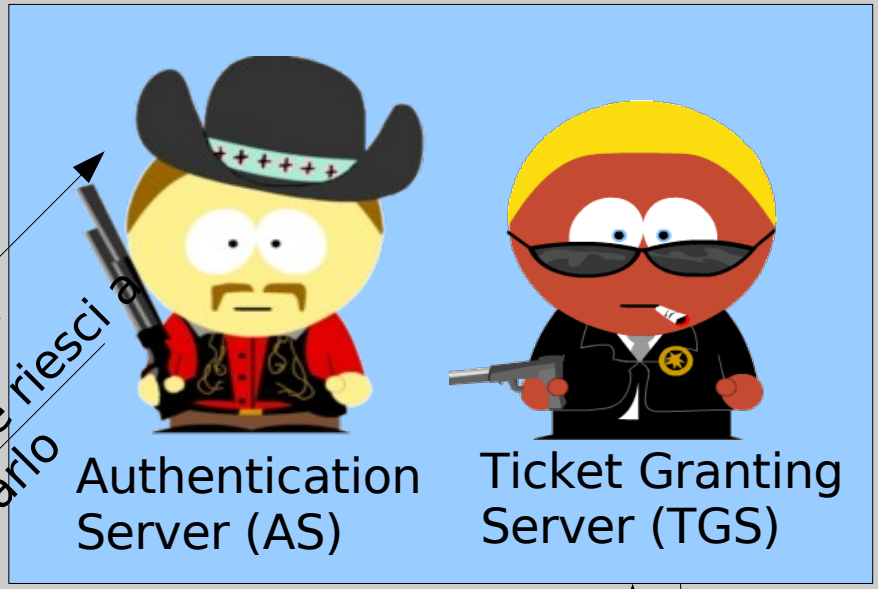


Utente

Networked Service

Single Sign On & Software Libero

Key Distribution Center (KDC)



1. Sono Alice, mi serve un TGT

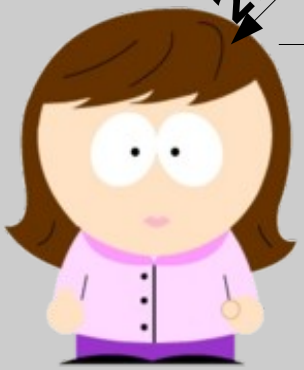
2. Ecco il TGT, se riesci a decriptarlo

3. TGT, voglio un Service Ticket

4. Ecco il Service Ticket

5. Autenticami, ho il Service Ticket

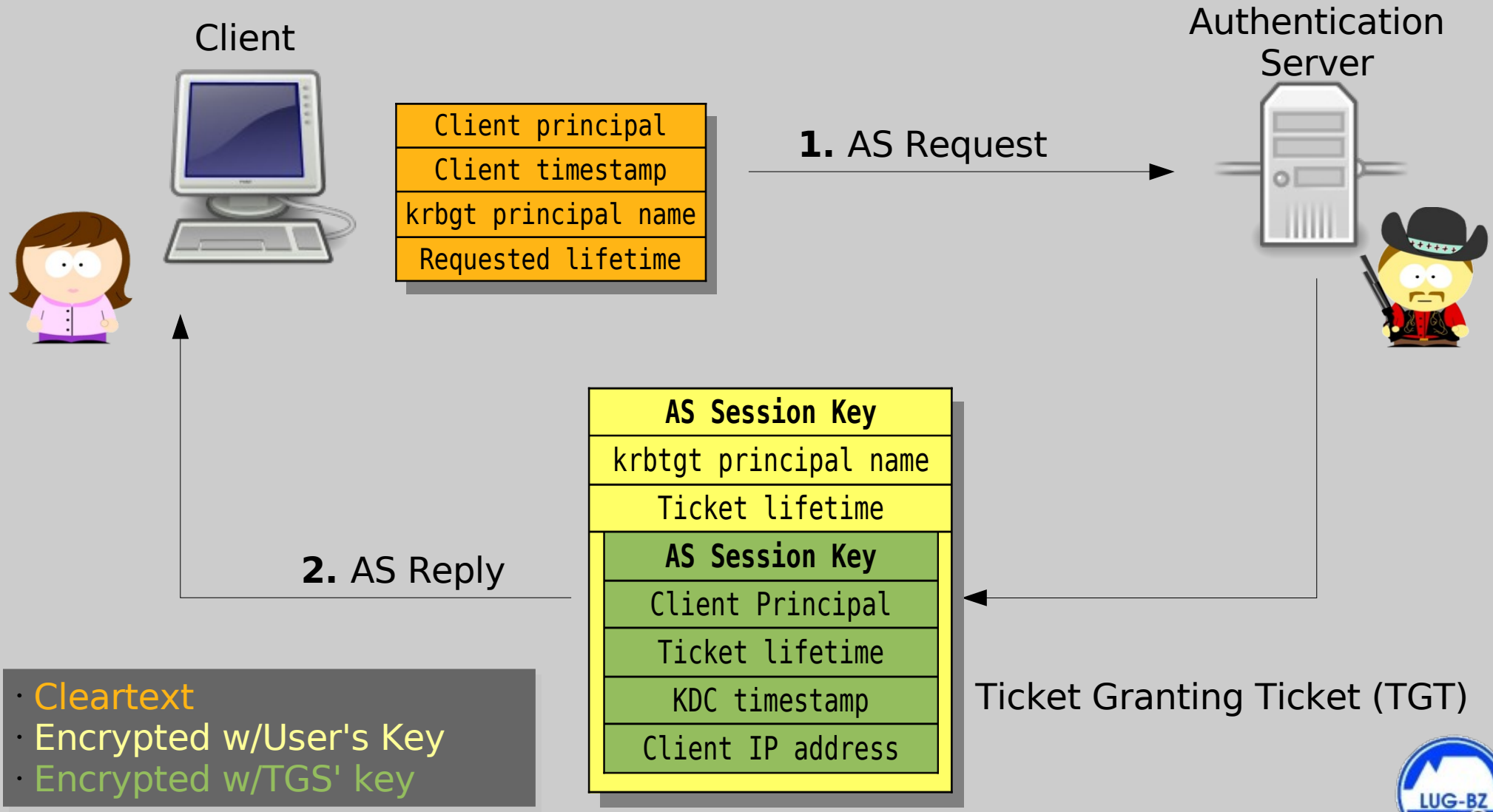
6. Ciao Alice, parliamo



Utente

Networked Service

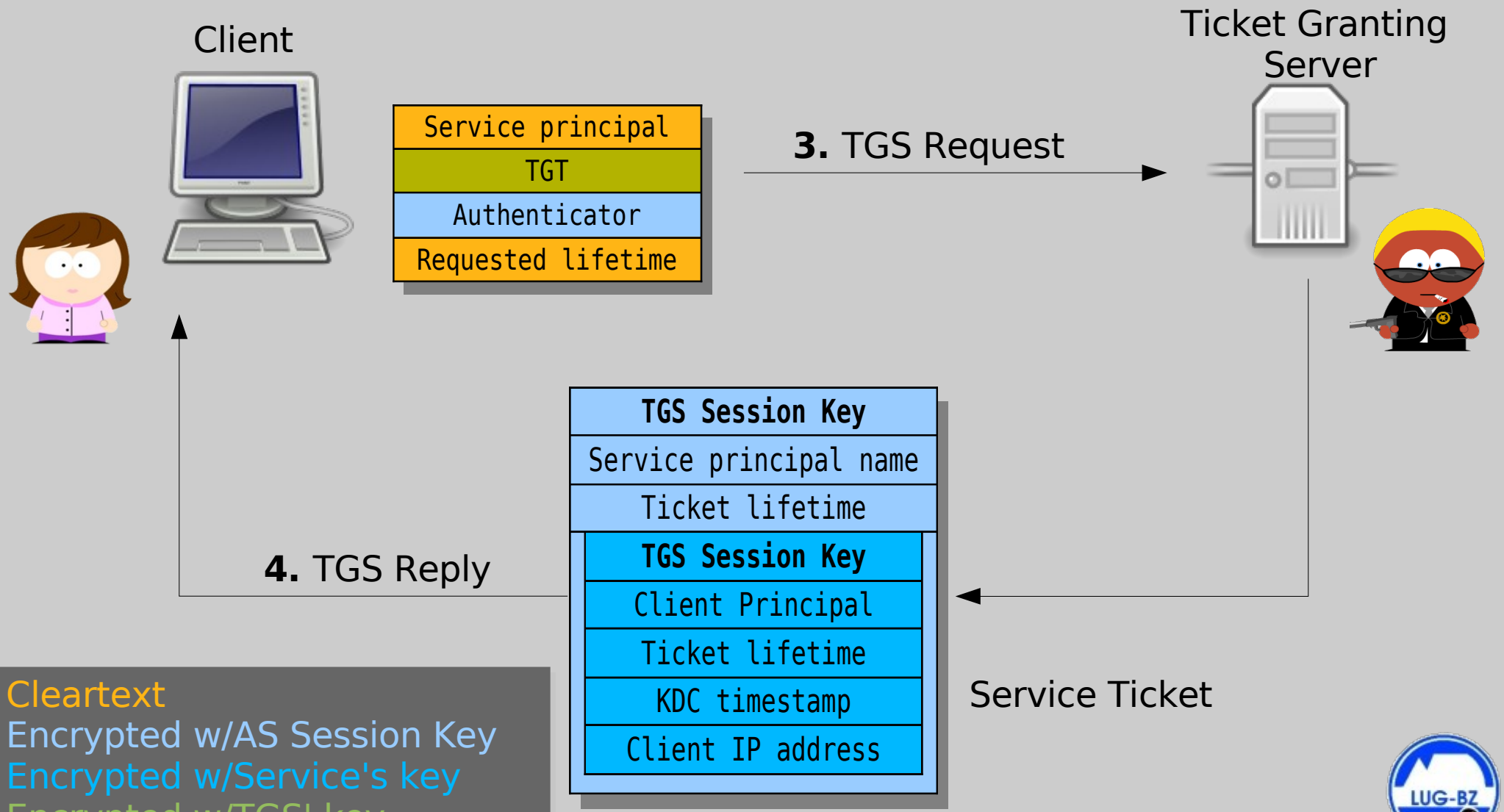
Single Sign On & Software Libero



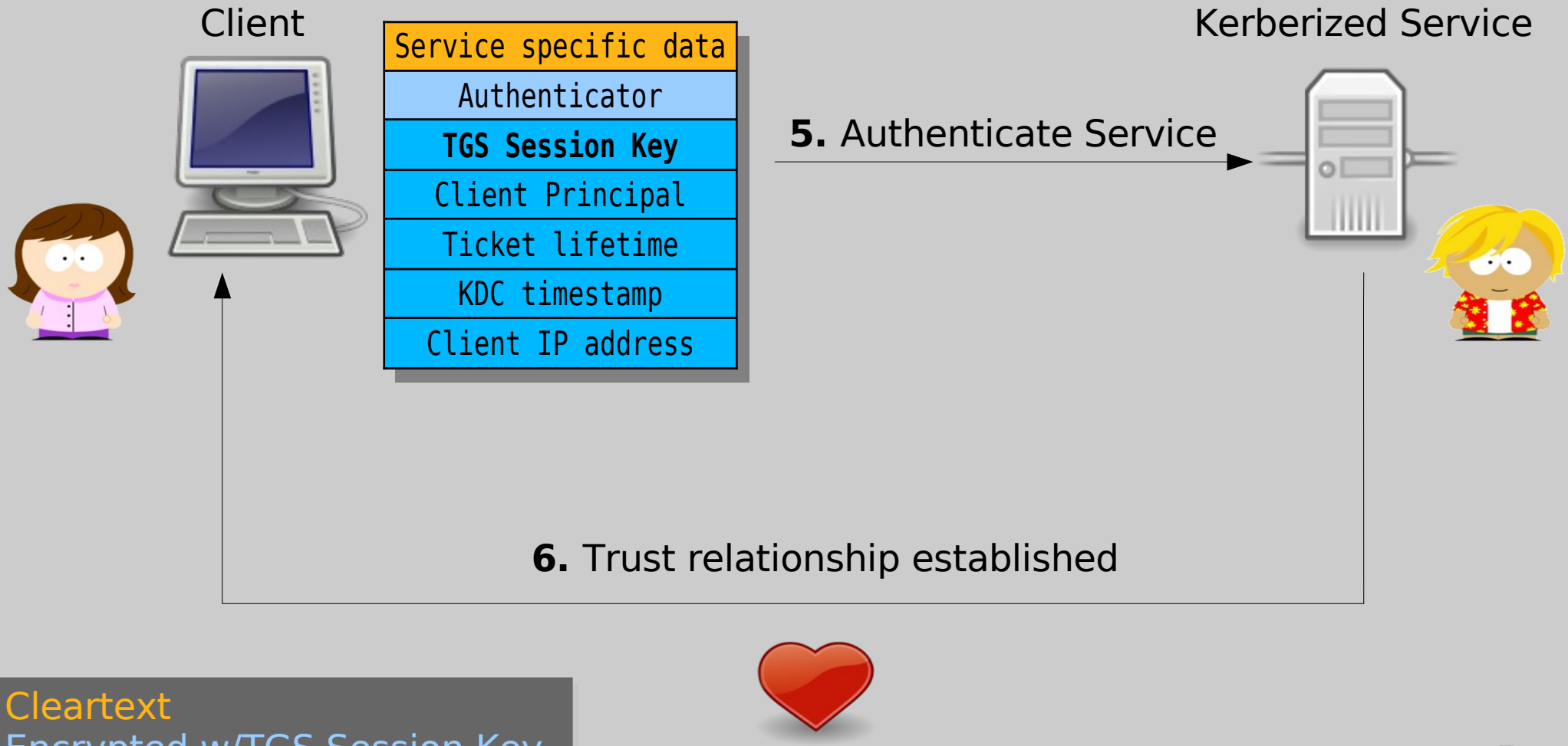
- Cleartext
- Encrypted w/User's Key
- Encrypted w/TGS' key

- *Session key* condivisa tra client e TGS
- Client memorizza nella *Credential Cache* la Session Key e il TGT

Single Sign On & Software Libero



Single Sign On & Software Libero



- Cleartext
- Encrypted w/TGS Session Key
- Encrypted w/Service's key

Single Sign On & Software Libero

- **Implementazioni esistenti**
- MIT Kerberos
  - Reference implementation
  - Supportato su molte piattaforme
  - API più utilizzate
  - *http://web.mit.edu/Kerberos/*

Single Sign On & Software Libero

- **Implementazioni esistenti (2)**
- Heimdal
  - Nato a causa delle restrizioni sulle esportazioni di crittografia vigenti negli USA anni fa)
  - Kerberos di default sui *BSD
  - Base Kerberos in Samba 4
  - *www.h5l.se*

Single Sign On & Software Libero

- **Implementazioni esistenti (3)**
- Active Directory
- E' un insieme di tecnologie (DNS, LDAP, RPC, ...) tra cui anche Kerberos
  - Presente da Windows 2000 in poi
  - Non supporta versioni più vecchie del protocollo kerberos (*kerberos 4*)
  - Ben integrata

Single Sign On & Software Libero

- **Pro**
- Maggiore produttività
- Maggiore sicurezza (password non viaggiano mai sulla rete, policy consistenti)
- Amministrazione semplificata
- Costi di gestione minori

Single Sign On & Software Libero

- **Contro**
- Una password compromessa dà accesso a tutti i sistemi (*strong authentication!*)
- Applicazioni devono essere *”kerberos-ready”*
- Funzionamento problematico in caso di NAT
- Distribuzione chiavi sui servizi
- Orologi devono essere sincronizzati
- Availability del/dei KDC cruciale

Single Sign On & Software Libero

- **Heimdal / Debian**
- Configurazione rete (NTP e DNS)
- KDC
- Client
- Server SSH
- Server HTTP
- Altri servizi

Single Sign On & Software Libero

- **Configurazione rete (NTP e DNS)**
- *kdc# apt-get install openntp bind9*

Single Sign On & Software Libero

- **KDC**

 # apt-get install heimdal-kdc heimdal-clients

- */etc/krb5.conf:*

```
[libdefaults]
        default_realm = LUGBZ.ORG
[realms]
        LUGBZ.ORG = {
                kdc = kdc.lugbz.org
                admin_server = kdc.lugbz.org
        }
[domain_realm]
        .lugbz.org = LUGBZ.ORG
        lugbz.org = LUGBZ.ORG
```

Single Sign On & Software Libero

KDC (2)

- Inizializzazione realm:

```
# kadmin -l

kadmin> init LUGBZ.ORG

Realm max ticket life [unlimited]:

Realm max renewable ticket life [unlimited]:
```

- Aggiunta utente admin:

```
kadmin> add michele/admin

Max ticket life [1 day]:

Max renewable life [1 week]:

Principal expiration time [never]:

Password expiration time [never]:

Attributes []:

michele/admin@LUGBZ.ORG's Password:
```

- Test autenticazione:

```
kdc# kinit michele/admin
kdc# klist
Credentials cache:
   FILE:/tmp/krb5cc_0
        Principal:
   michele/admin@LUGBZ.ORG
  Issued           Expires
     Principal
May 20 13:15:54  May 20 23:15:54
   krbtgt/LUGBZ.ORG@LUGBZ.ORG
```

Single Sign On & Software Libero

KDC (3)

- Aggiunta di *michele/admin* come amministratore Kerberos *(/etc/heimdal-kdc/kadmind.acl – attivare kadmin in inetd)* per poter amministrare anche da remoto:

michele/admin@LUGBZ.ORG all

```
# kinit michele/admin

# kadmin

kadmin> list *
```

- Aggiunta utente non amministrativo:

```
kadmin> add michele
```

Single Sign On & Software Libero

Client

 # apt-get install heimdal-clients openssh-client libpam-krb5

- Configurazione PAM:

/etc/pam.d/common-auth:

auth sufficient pam_krb5.so forwardable

auth sufficient pam_unix.so nullok_secure use_first_pass

/etc/pam.d/common-password:

password sufficient pam_krb5.so use_authtok

password sufficient pam_unix.so nullok ...

- Va creato l'utente *michele* senza password (andrebbe usato LDAP per centralizzare anche le informazioni su utenti e gruppi)
- Per testarlo basta, loggarsi alla console e verificare di aver ottenuto il ticket con il comando *klist*

Single Sign On & Software Libero

Server (SSH)

krb-server.lugbz.org

 # apt-get install openssh-server heimdal-clients

- Creiamo e installiamo tramite kadmin remoto la chiave del principal per SSH

 # kinit michele/admin; kadmin

*kadmin> add --random-key **host/krb-server.lugbz.org***

kadmin> ext_keytab -k /etc/krb5.keytab host/krb-server.lugbz.org

- Aggiungere l'utente *michele* e configurare SSH in modo appropriato :

KerberosAuthentication yes

KerberosOrLocalPasswd yes

KerberosTicketCleanup yes

GSSAPIAuthentication yes

GSSAPICleanupCredentials yes

- Dal client, *ssh michele@krb-server.lugbz.org* e ci si autentica ”passwordless” :

May 20 18:09:28 krb-server sshd[4640]: Authorized to michele, krb5 principal michele@LUGBZ.ORG (krb5_kuserok)

Single Sign On & Software Libero

Server (HTTP)

krb-server.lugbz.org

 # apt-get install libapache2-mod-auth-kerb apache2-mpm-prefork

- Creiamo il keytab con la chiave per Apache e lo esportiamo:

*kadmin> add -r **HTTP/krb-server.lugbz.org***

Max ticket life [1 day]:

Max renewable life [1 week]:

Principal expiration time [never]:

Password expiration time [never]:

Attributes []:

kadmin> ext_keytab -k /etc/apache2/apache.keytab HTTP/krb-server.lugbz.org

Single Sign On & Software Libero

Server (HTTP/2)

krb-server.lugbz.org

- Creiamo il virtual host:

```
<Directory /var/www/secret>
        Options Indexes SymlinksIfOwnerMatch
        AuthType Kerberos
        AuthName "LUGBZ.ORG Login"
        Krb5Keytab /etc/apache2/apache.keytab
        KrbAuthRealms LUGBZ.ORG
        KrbSaveCredentials on
        require valid-user
</Directory>
```

- Firefox richiede modifiche a *network.negotiate-auth.trusted-uris* se non si usa SSL

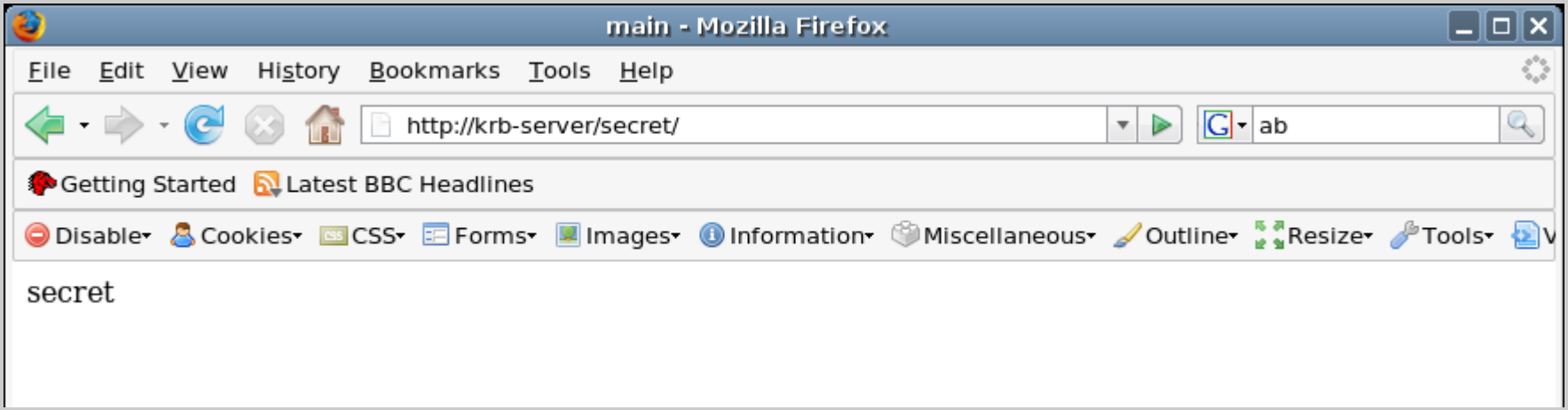
Single Sign On & Software Libero

Server (HTTP/3)

- Otteniamo i ticket:

krb-server.lugbz.org

- E ci colleghiamo con firefox:



Single Sign On & Software Libero

- **Altri servizi**
- OpenLDAP / FDS (LDAP)
- Dovecot (POP / IMAP)
- Postfix (SMTP)
- Postgresql
- Cyrus IMAP
- OpenSSH
- Apache HTTP
- Jabber
- NFSv4

Single Sign On & Software Libero

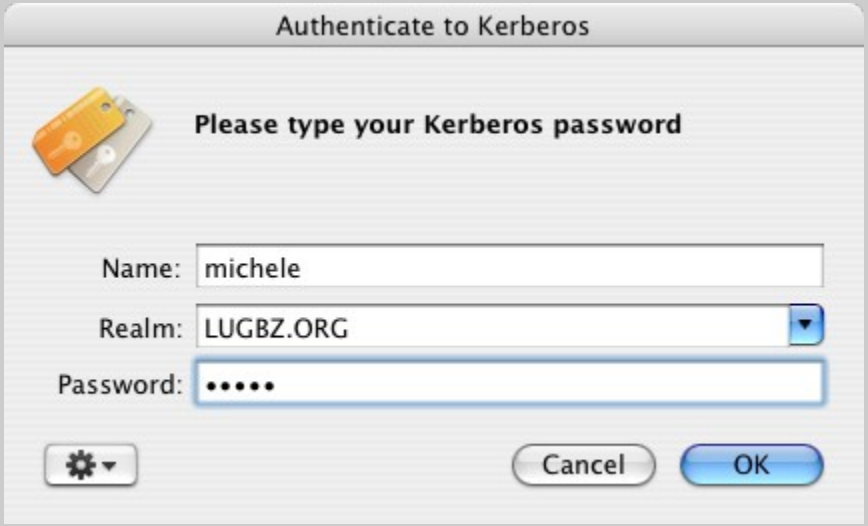
- **Altri servizi (2)**
- Squid
- AFS
- ftp
- telnet
- Cups / IPP (sperimentale)
- SNMP (draft)
- ...

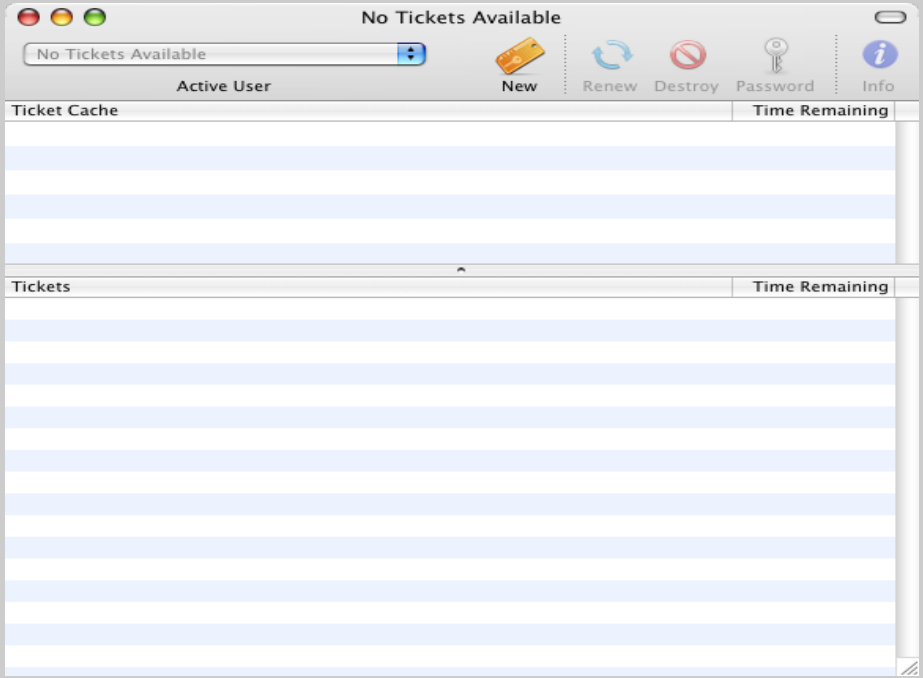
Single Sign On & Software Libero

- **Integrazione con altri S.O.**
- *NIX
  - MIT
  - Heimdal
  - GNU Shishi

Single Sign On & Software Libero

- **Integrazione con altri S.O. (2)**
- Mac OS X
  - Librerie Kerberos MIT
  - Login con autenticazione Kerberos





Single Sign On & Software Libero

- **Integrazione con altri S.O. (3)**
- Microsoft Windows
  - Windows 2000 in poi
  - Senza supporto nativo AD, è limitato (solo utenti locali)
  - Necessita di installazione tool aggiuntivi (*ksetup.exe* e *klist.exe* dal Resource Kit di Windows)

Single Sign On & Software Libero

- **Integrazione con altri S.O. (4)**
- Creare un host principal (*host/win-client1.lugbz.org*) sul KDC

net time /SETSNTP:kdc.lugbz.org

ksetup /SetDomain LUGBZ.ORG

ksetup /SetMachPassword <password>

ksetup /AddKdc LUGBZ.ORG kdc.lugbz.org

ksetup /AddKpasswd /AddKpasswd LUGBZ.ORG kdc.lugbz.org

*ksetup /mapuser * **

Single Sign On & Software Libero

- **Il futuro**
- Samba 4
- Heimdal 0.8 / MIT 1.7
- PK-INIT
- Kerberize your app today

Single Sign On & Software Libero

Grazie dell'attenzione

St IGNUcius be with you