secureendpoints

NIST PKI'06:
Integrating PKI and Kerberos (updated April 2007)

Jeffrey Altman

The Slow Convergence of PKI and Kerberos

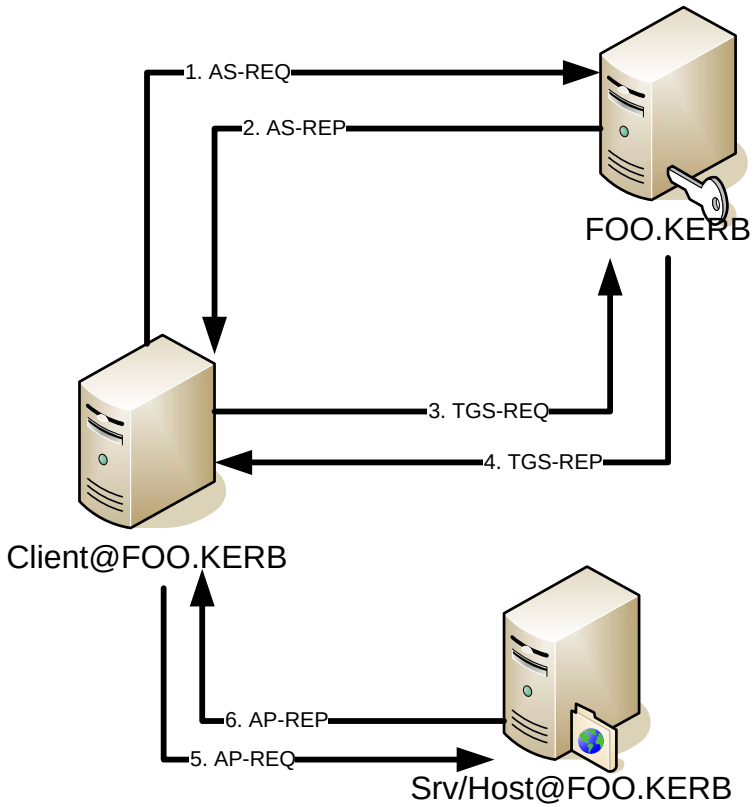
- At Connectathon 1995 Dan Nessett of Sun Microsystems was quoted saying “Kerberos will gradually move toward public-key” in reference to the publication of Internet Draft
  - **draft-ietf-cat-kerberos-pk-init-00**
- IETF CAT Working Group (Apr 1995) discussed not only pk-init-00 but also Netscape’s proposal for something called SSL.
- Eleven years and 34 drafts later PK-INIT was approved as an IETF Proposed Standard (RFC 4556)

How much more gradually can we move? ☺

secureendpoints

A Three Slide Overview of Kerberos V5 Before PKI: Single Realm

- The Authentication Service (AS) Exchange
  - The client obtains an "initial" ticket from the Kerberos authentication server (AS), typically a Ticket Granting Ticket (TGT).
  - The AS-REQ may optionally contain pre-authentication data to prove the client's identity.
  - The AS-REP, containing an authenticator (aka ticket), is encrypted in the client's long term key.
- The Ticket Granting Service (TGS) Exchange
  - The client subsequently uses the TGT to authenticate and request a service ticket for a particular service, from the Kerberos ticket-granting server (TGS).
- The Client/Server Authentication Protocol (AP) Exchange
  - The client then makes a request with an AP-REQ message, consisting of a service ticket and an authenticator that certifies the client's possession of the ticket session key. The server may optionally reply with an AP-REP message. AP exchanges typically negotiate session specific symmetric keys.



secureendpoints

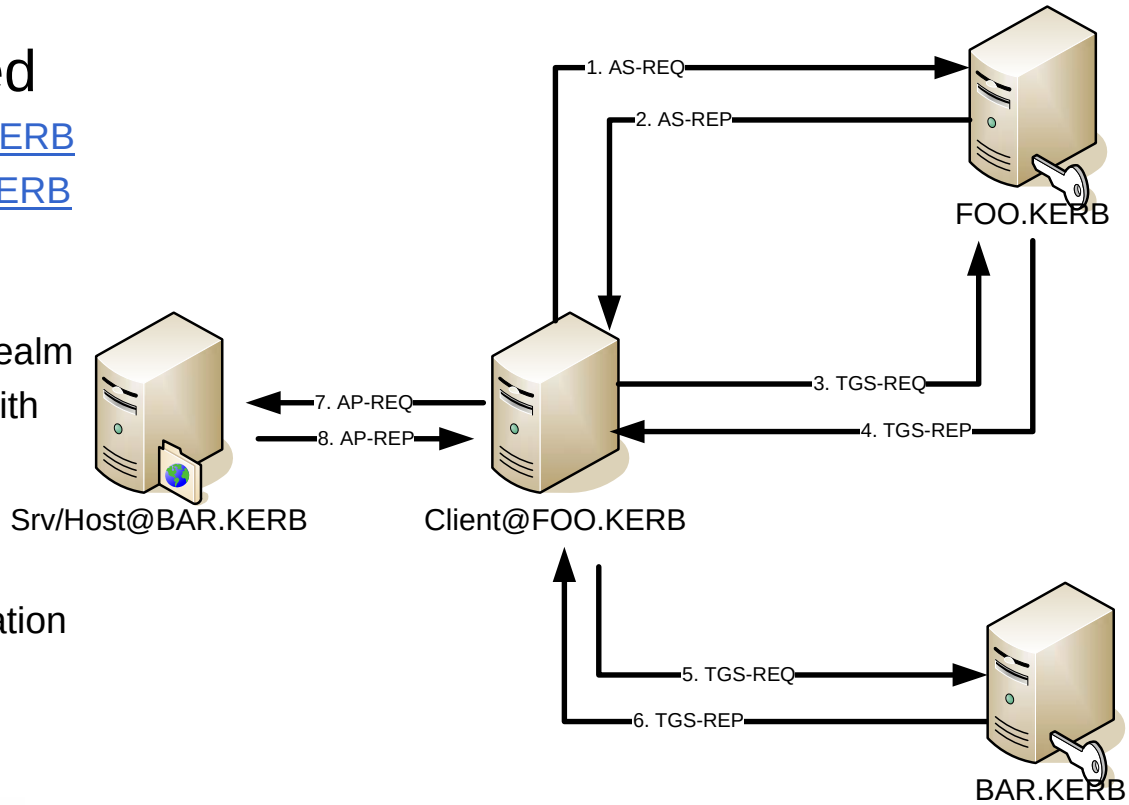
Slide 2: Kerberos 5 Cross Realm

Tickets Obtained

krbtgt/FOO.KERB@FOO.KERB
krbtgt/BAR.KERB@FOO.KERB
Srv/Host@BAR.KERB

Cross Realm works when realm FOO.KERB shares a key with realm BAR.KERB.

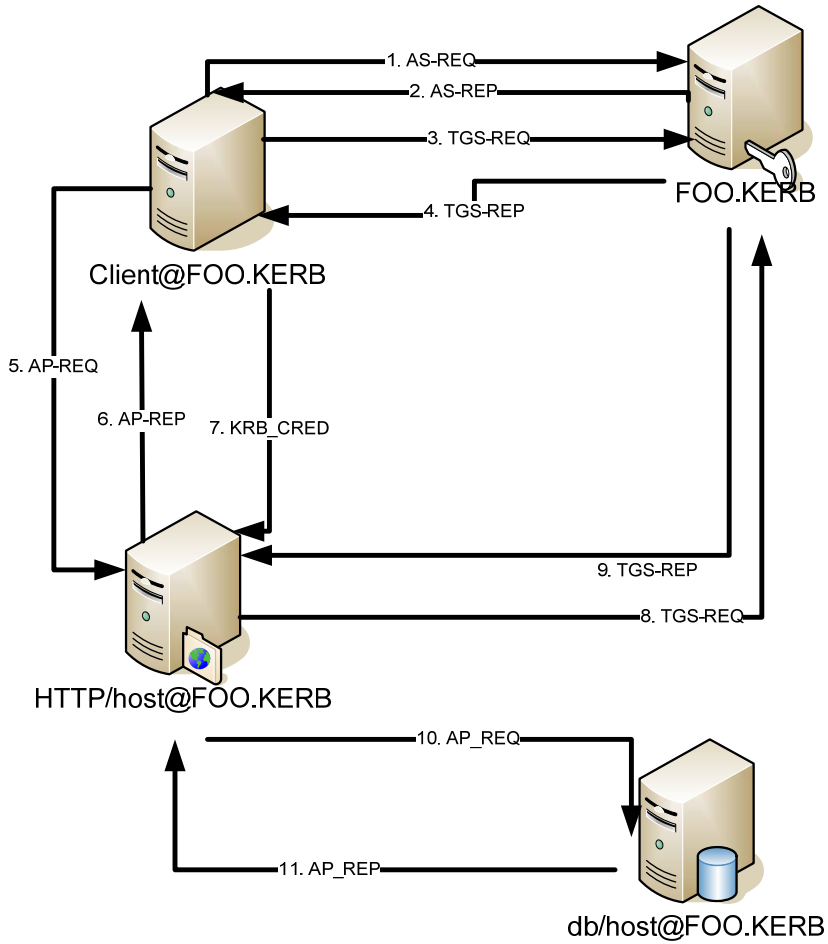
In all cases, the KDC must share a key with the application Service.



secureendpoints

Slide 3: Kerberos 5 Delegation

- Delegation utilizes the ability to FORWARD tickets from a client machine to a service.
- The service can then assume the identity of the client in order to authenticate to a subsequent service.
- Constraints can be applied to the forwarded tickets using authorization data.



secureendpoints

PKI and Kerberos have each excelled in separate but overlapping spheres

PKI and the Web

- Smartcards for logon
- Web Service authentication
- TLS authenticated services
  - FTP, SMTP, IMAP, many more …
- Signatures and Privacy (S/MIME)
  - E-mail
  - Instant Messages

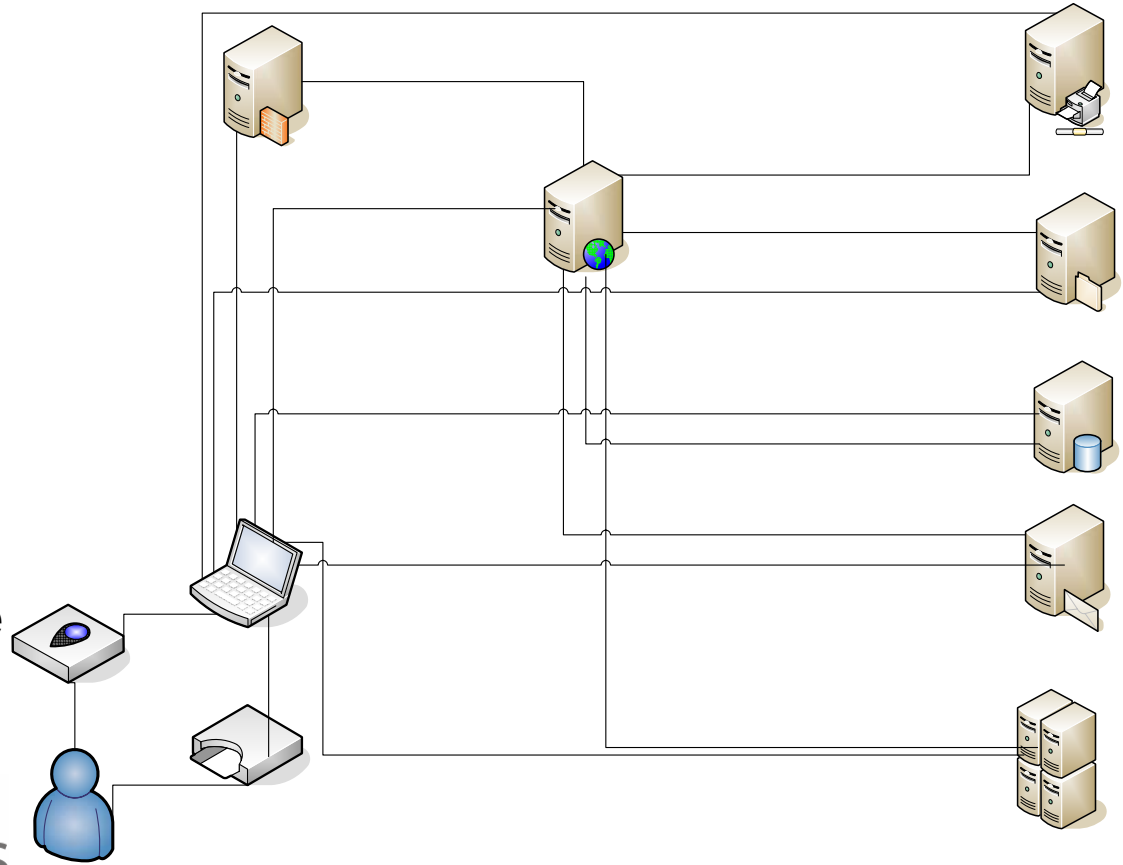
Kerberos and Enterprise Services

- Console Logon
- Remote Console Logon
- File System Access
  - AFS, NFS, CIFS, FTP
- E-mail Service Access
- Print Services
- Real-time authenticated messaging
  - Zephyr

But combining PKI and Kerberos is necessary for true Single Sign-On

- Multifactor Initial Authentication
- Mutual Client Server authentication
- With Delegation
- Through Proxies
- Supporting all protocols

It's a big task but we can do it!!!



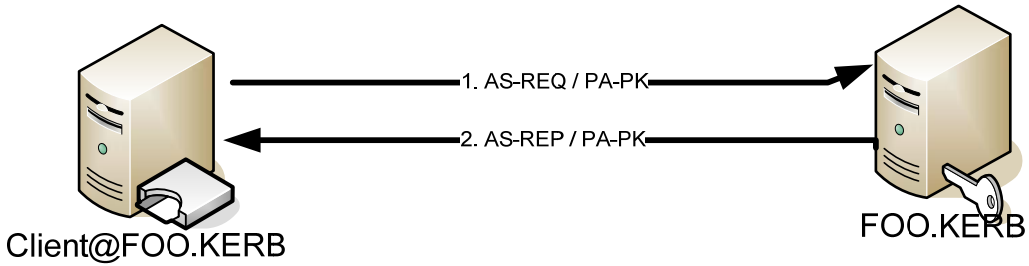
secureendpoints

How the PKI and Kerberos worlds can be joined

- Imagine a world in which each Kerberos Key Distribution Center is also a Certificate Authority.
  - Its not hard to do, think Microsoft Active Directory.
- PK-INIT*
  - Kerberos Initial Ticket Acquisition using Public Key
    - Certificates or Raw Key Pairs
- PK-CROSS
  - Establishment of Kerberos Cross Realm relationships using Public Key
    - Mutual Authentication of KDCs
    - Secure Generation of Static Keys
- PK-APP (aka kx509/kca)*
  - Acquisition of Public Key certificates via Kerberized Certificate Authorities

*implementations are currently available

PK-INIT: How does it work?



- PK-INIT is implemented as a Kerberos Pre-authentication mechanism
- If the client's request adheres to KDC policy and can be validated by its trusted CAs, then the reply is encrypted either with
  - A key generated by a DH key exchange and signed using the KDC's signature key, or
  - A symmetric encryption key, signed using the KDC's signature key, and then encrypted with the client's public key.
- Any required keying material is returned to the client as part of the AS-REP's PA-PK data.
- If the client can validate the KDC's signature, obtain the encryption key, and decrypt the reply, then it has successfully obtained an Initial Ticket Granting Ticket.

secureendpoints

PK-INIT: Not Vaporware

- Draft -9 deployed by Microsoft in Windows 2000 and above
- The Proposed Standard (RFC 4556) is being deployed today:
  - Microsoft Vista
  - Heimdal Kerberos
- Future deployments:
  - MIT Kerberos 1.7 and the operating systems that distribute it

secureendpoints

PK-INIT: Opening the doors to alternative enrollment models

- Trusted CA issued certificate can be enrolled with multiple realms
- Raw public key pairs can be used instead of certs allowing SSH style enrollments
- A single smart card can be enrolled with multiple realms allowing the acquisition of TGTs for multiple service providers

secureendpoints

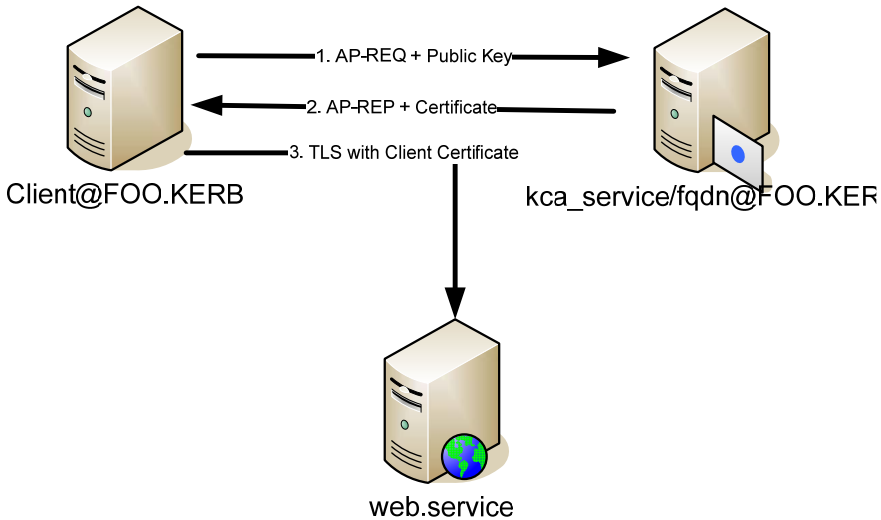
PK-CROSS: Easing the administrative challenges to key exchange

- Kerberos Cross Realm succeeds in Active Directory Forests because the key establishment is automated
- Kerberos Cross Realm works for the major Universities and Government labs because they have taken the time to manually establish keys
- For the rest of us, an automated key establishment protocol is required. Public key crypto could reduce the administrative burden to the configuration of policy.

secureendpoints

KX.509 (or How to authenticate using a Kerberos identity to a PKI service)

- KX509 utilizes a Kerberos Application Service authentication to communicate with a special certificate service that issues client certificates with the same identity and valid lifetime as the Kerberos Service ticket.
- The resulting certificate is placed in the certificate store for use by applications such as web browsers.



secureendpoints

What's Next for Kerberos and PKI Integration?

- Standardize PK-CROSS and PK-APP (kx509/kca)
- Strive for Zero Configuration
- Standardize the use of SAML decoration of PKI Certificates and Kerberos Tickets
- Standardize a firewall friendly method of communicating with Kerberos KDCs
  - Microsoft and Secure Endpoints are co-authoring IAKERB, a proxy mechanism that permits Kerberos TGS requests to be tunneled as part of a GSS-API service authentication
- Improve the user experience
  - Focus deployment efforts on the goal of reducing the number of credentials end users are responsible for securing

References

- KX509/Kerberized Certificate Authority
  http://www.kx509.org
- IETF Kerberos Working Group
  http://www.ietf.org/html.charters/krb-wg-charter.html
- Heimdal PKINIT
  http://people.su.se/~lha/patches/heimdal/pkinit/
- Microsoft Windows 2000 PKINIT
  http://support.microsoft.com/kb/248753/en-us

secureendpoints

Q & A

Requirements for Federated Single Sign-On

- Trusted initial authentication
  - Smartcards, Zero Knowledge Inference, Biometrics, One Time Pads.
  - May require different methods depending on the environment
- Mutual Authentication between each set of endpoints
- Delegation of credentials with constraints
  - Forwardable Kerberos tickets
  - Authorization Data (MS PAC, SAML) provide constraints
- Ability to present a recognizable credential to each service
  - Certificates or Tickets
- Federated acceptance of presented credentials

secureendpoints