Kerberos for Internet-of-Things

IETF89

Thomas Hardjono
MIT Kerberos & Internet Trust Consortium

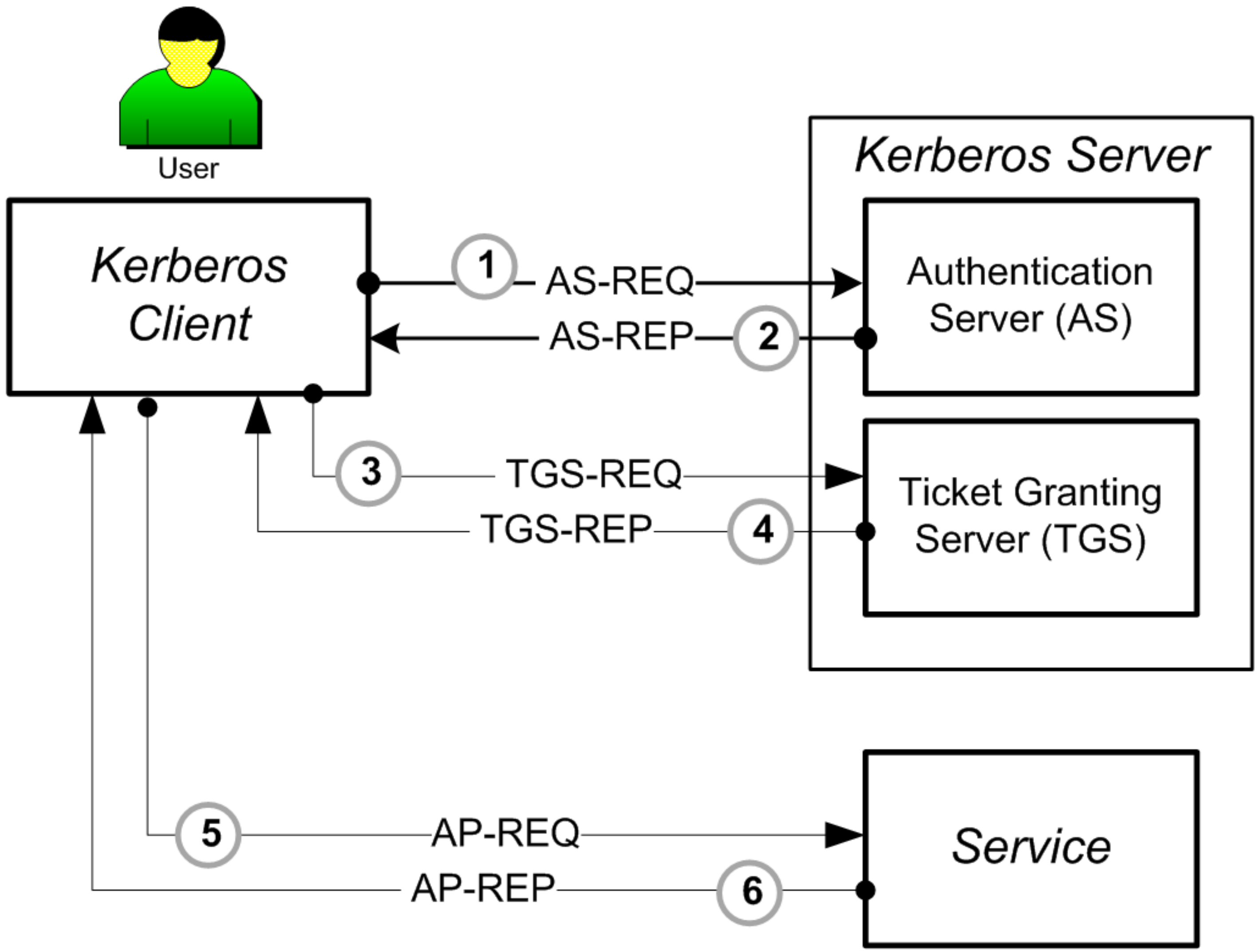
February, 2014

Contents

- Kerberos Protocol Overview
- Kerberos in Devices
  - DOCSIS & PacketCable
  - Intel AMT
- Kerberos for IoT (pros & cons)
- History of Kerberos

Kerberos Protocol Overview

Kerberos Protocol Messages



Needham-Schroeder Protocol

$$A \rightarrow S : A, B, N_a$$

$$S \rightarrow A : \{N_a, B, K_{ab}, \{K_{ab}, A\}_{K_{bs}}\}_{K_{as}}$$

$$A \rightarrow B : \{K_{ab}, A\}_{K_{bs}}$$

$$B \rightarrow A : \{N_b\}_{K_{ab}}$$

$$A \rightarrow B : \{N_b - 1\}_{K_{ab}}$$

- S is Server (KDC)
- A and B are Client and Service
- N is nonce
- K is the shared symmetric key

MIT KIT INTERNET TRUST

Basic Flows

- Long term symmetric keys:
  - Client and KDC share unique long-term key
  - Service and KDC share unique long term key
- Long term keys used to establish session-keys
  - Used to encrypt Tickets & Authenticators
  - Ticket-Granting-Ticket (TGT) and Service Ticket
- Authenticator:
  - Encrypted by Client to provide *Proof-of-Possession* (POP) to intended recipient

What's Inside a Ticket Granting Ticket

Ticket (Ticket Granting Ticket (TGT))

Ticket version No.	[tkt-vno]
Issuing Server's Realm	[realm]
Server's Principal Name	[sname]
Encrypted Ticket Part	[enc-part]

Ticket Flags	[flags]
Session Encryption Key	[key]
Client's Realm	[crealm]
Client's Principal Name	[cname]
Transited Realms	[transited]
Time of initial authentication	[authtime]
Start Time of ticket (opt)	[starttime]
Expiration Time of ticket	[endtime]
Max renew time of ticket (opt)	[renew-till]
Client Host Addresses (opt)	[caddr]
Restrictions (opt)	[authorization-data]

MIT INTERNET TRUST

What's Inside a Service Ticket

Ticket (Service Ticket)

Ticket version No.	[tkt-vno]
Issuing Server's Realm	[realm]
Server's Principal Name	[sname]
Encrypted Ticket Part	[enc-part]
Ticket Flags	[flags]
Session Encryption Key	[key]
Client's Realm	[crealm]
Client's Principal Name	[cname]
Transited Realms	[transited]
Time of initial authentication	[authtime]
Start Time of ticket (opt)	[starttime]
Expiration Time of ticket	[endtime]
Max renew time of ticket (opt)	[renew-till]
Client Host Addresses (opt)	[caddr]
Restrictions (opt)	[authorization-data]

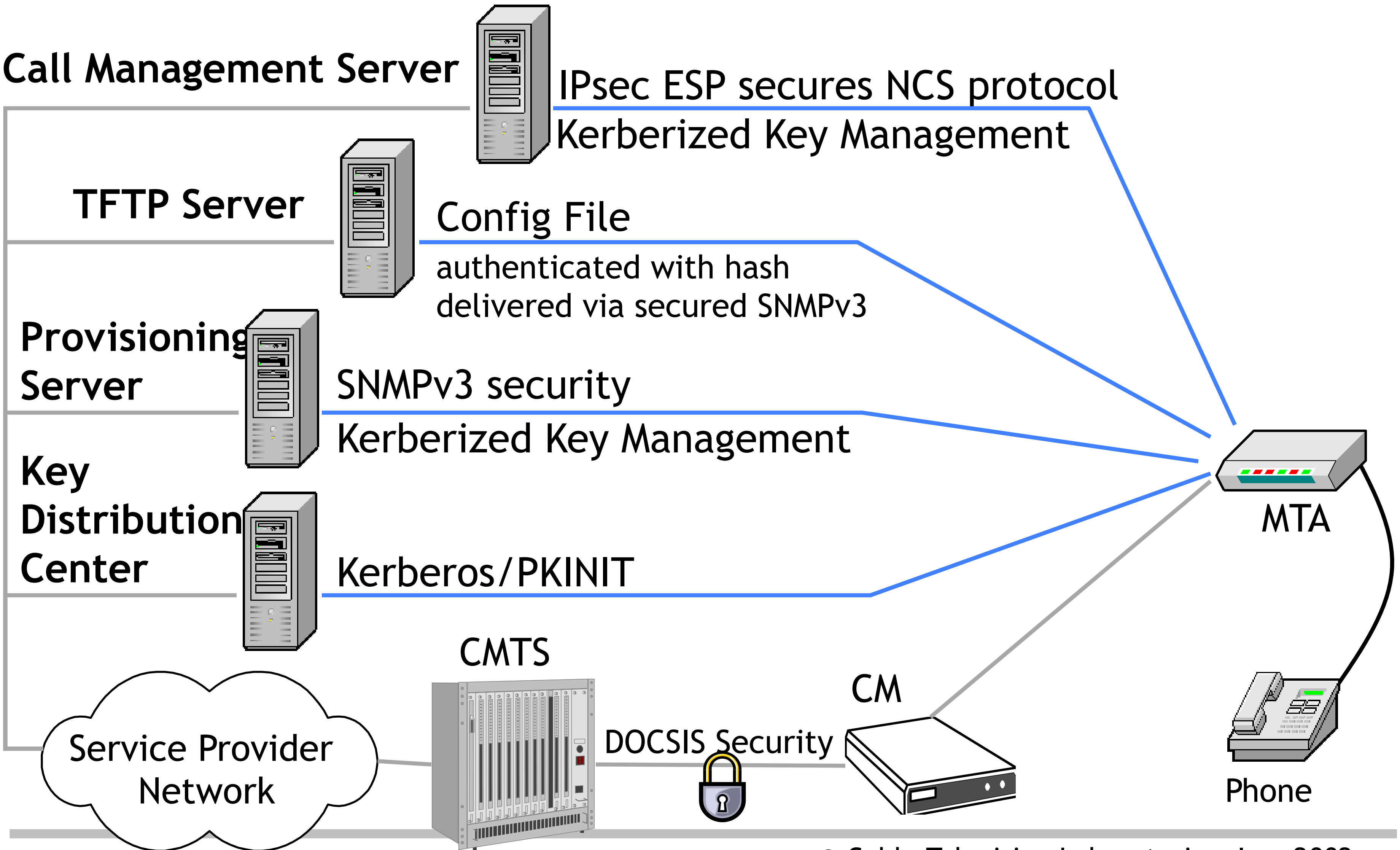
What’s Inside an Authenticator

Authenticator

Authenticator version No.	[authenticator-vno]
Client's Realm	[realm]
Client's Principal Name	[cname]
Checksum (opt)	[cksum]
Client's time/microsecs	[cusec]
Client's current time	[ctime]
Sub-key (opt)	[subkey]
Sequence Number (opt)	[seq-number]
Authorization data (opt)	[authorization-data]

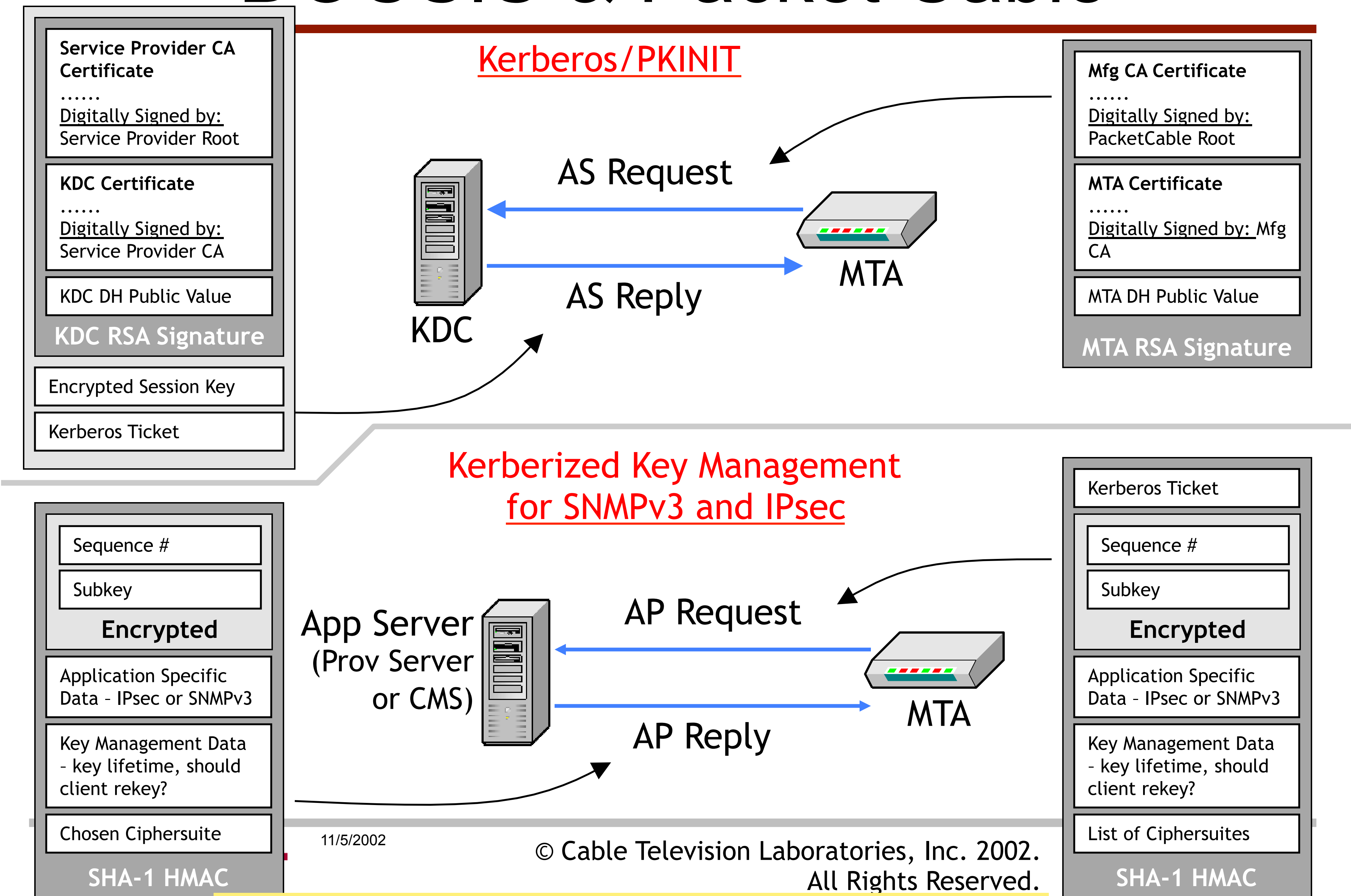
Kerberos in Devices & Embedded Systems

DOCSIS & Packet Cable



Packet Cable 1.5 (PKT-SP-PROV1.5-I04-090624)

DOCSIS & Packet Cable



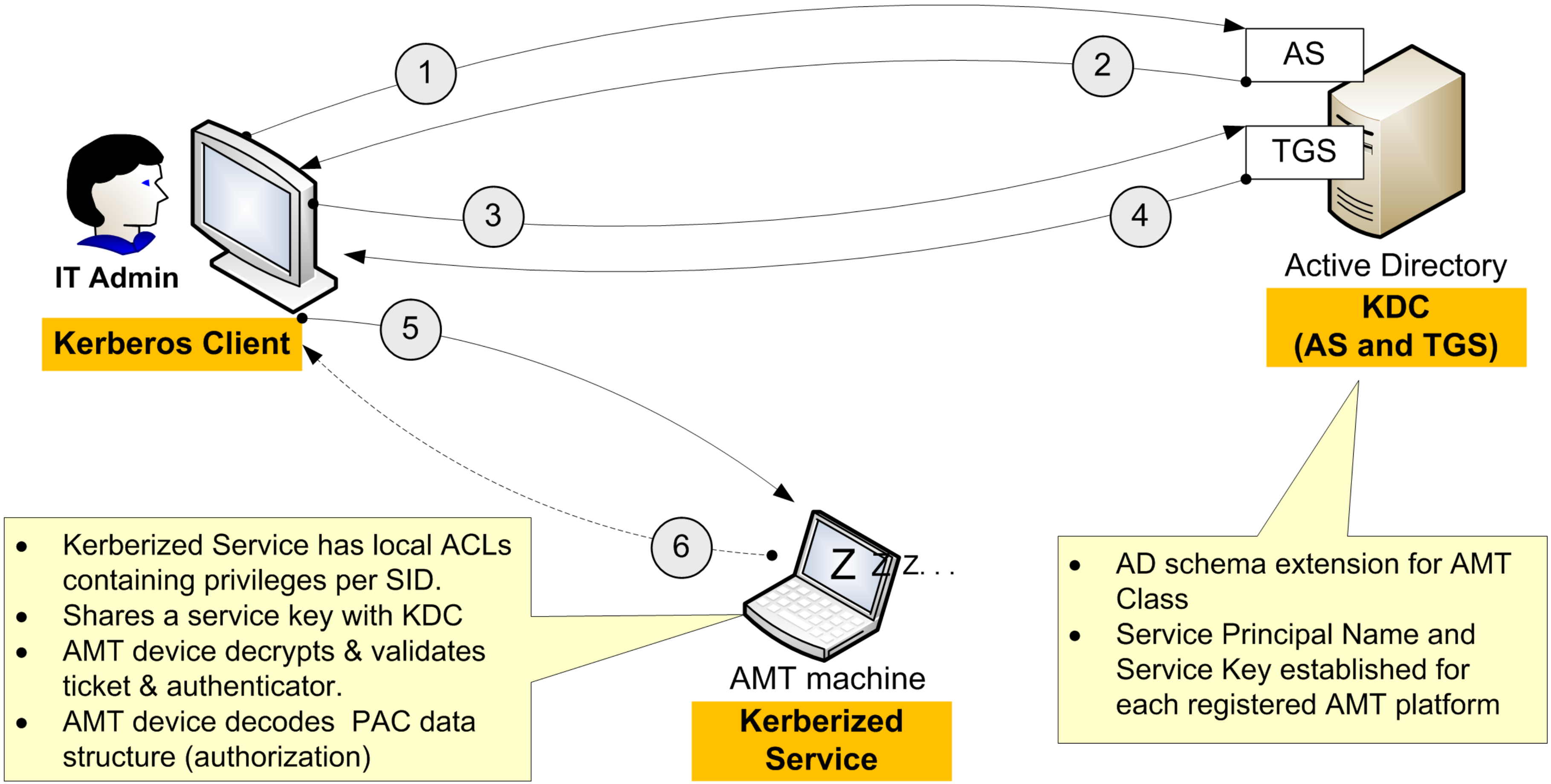
Packet Cable 1.5 (PKT-SP-SEC1.5-I03-090624)

Kerberos in Intel® AMT

- Active Management Technology (AMT)
  - Manageability technology for Intel platforms (hardware, firmware, software)
- Out-of-Band Manageability:
  - OS-independent (i.e. Pre-OS) & runs on auxiliary power
  - Remote boot (Serial-over-LAN)
  - Remote diagnostics & firmware updates (pre-OS boot)
  - Remote OS repairs
  - Bound to PC hardware (difficult to tamper)
- IT Administrator <u>must be authenticated</u> by AMT device before performing AMT operations remotely

MIT KIT INTERNET TRUST

Kerberos in Intel® AMT



Other Embedded Case Studies

- See TeamF1 presentation:
  - Data Center authentication
  - VPN termination device
  - Industrial automation

http://www.kerberos.org/events/2009conf/TeamF1.pdf

Kerberos.org and Other Links

- Needham-Schroeder paper (1978):
  - "Using encryption for authentication in large networks of computers.". *CACM* **21** (12): 993–999.
  - Also see Denning-Sacco paper (1981) *CACM* **24** (8): 533–535
- Kerberos RFC 4120:
  - https://www.ietf.org/rfc/rfc4120.txt
- MIT Code Base distribution (now Rel 1.12)
  - http://web.mit.edu/kerberos/dist/
- Kerberos APIs documentation:
  - http://web.mit.edu/kerberos/krb5-current/doc/
- Some Guides:
  - http://www.kerberos.org/software/whitepapers.html

MIT KIT INTERNET TRUST

Kerberos in Constrained Devices

Kerberos for IoT: the *Pros*

- Well understood protocol (cf. Needham-Schroeder)
- Symmetric-key approach suits constrained devices
  - Long-term keys can be installed by device manufacturer
  - Symmetric key operations cheaper/faster
  - Kerberos flows can be optimized for IoT devices
- Integration with directories a well-trodden path
- Open source code (20+ years)
  - MIT code written in C – several generations of coders
  - Active dev community

MIT KIT INTERNET TRUST

Kerberos in IoT: the *Cons*

- RFC4120 will put you to sleep…☺
- No initial key distribution protocol
  - Use PKINIT (RFC6112) or similar
- Good C programmers hard to come-by

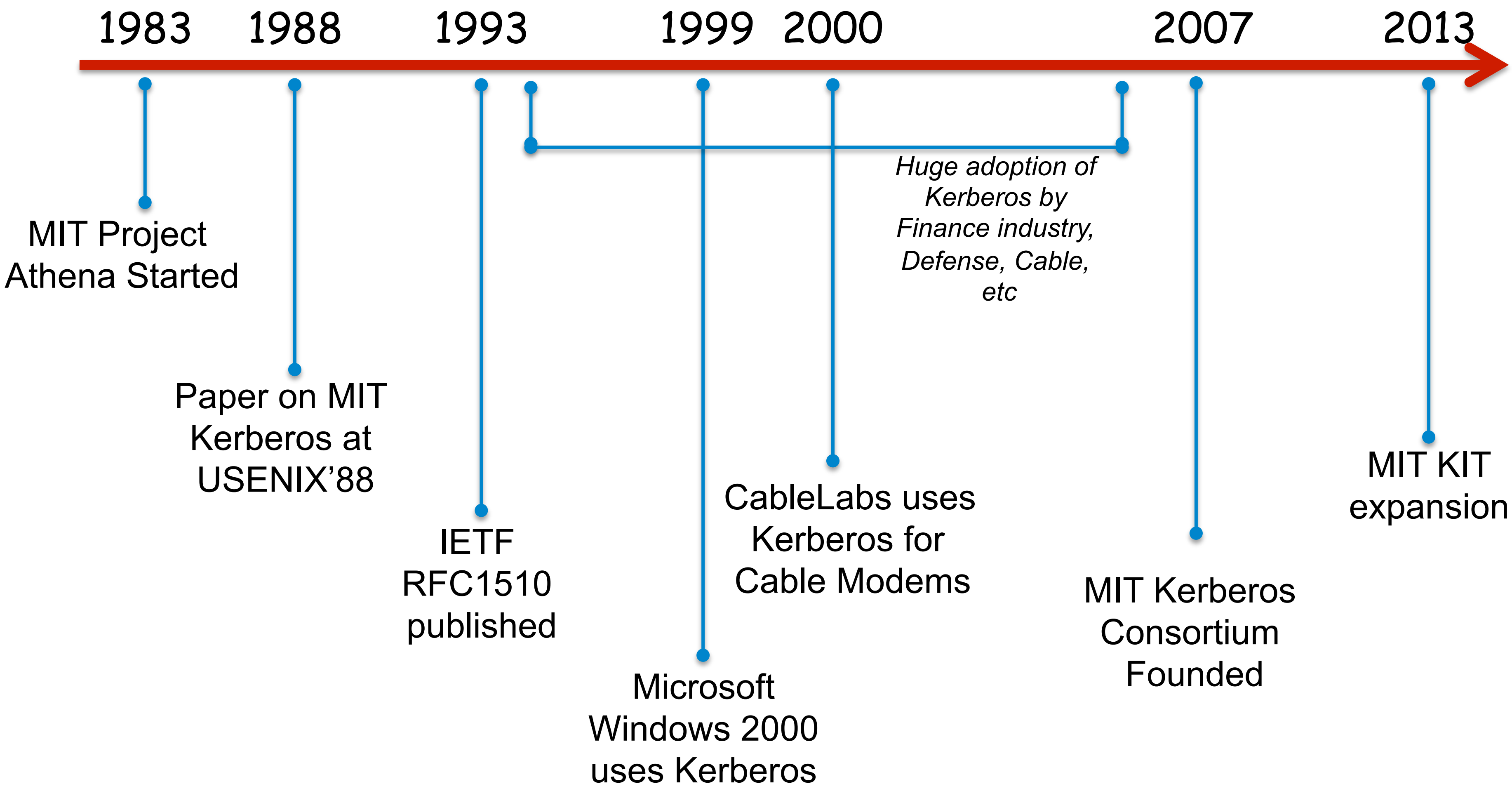
Kerberos History & Status

A Brief History of Kerberos

- Kerberos was developed as the Authentication engine for MIT's Project Athena in 1987:
  - Became IETF standard in 1993 (RFC1510) – now RFC4120
- MIT's release of Kerberos as open source in 1987 led to rapid adoption by numerous organizations
- Kerberos now ships standard with *all* major operating systems
  - Apple, Red Hat, Microsoft, Sun, Ubuntu
- Serves tens of millions of enterprise users:
  - Microsoft has been using Kerberos as the default authentication package since Windows 2000
  - Windows Logon used daily by millions of users.
  - Used in DOCSIS CableModems for device authentication.
  - Used for embedded systems security
- Kerberos has been *hugely* successful

MIT KIT INTERNET TRUST

MIT Kerberos: Timeline & Milestones



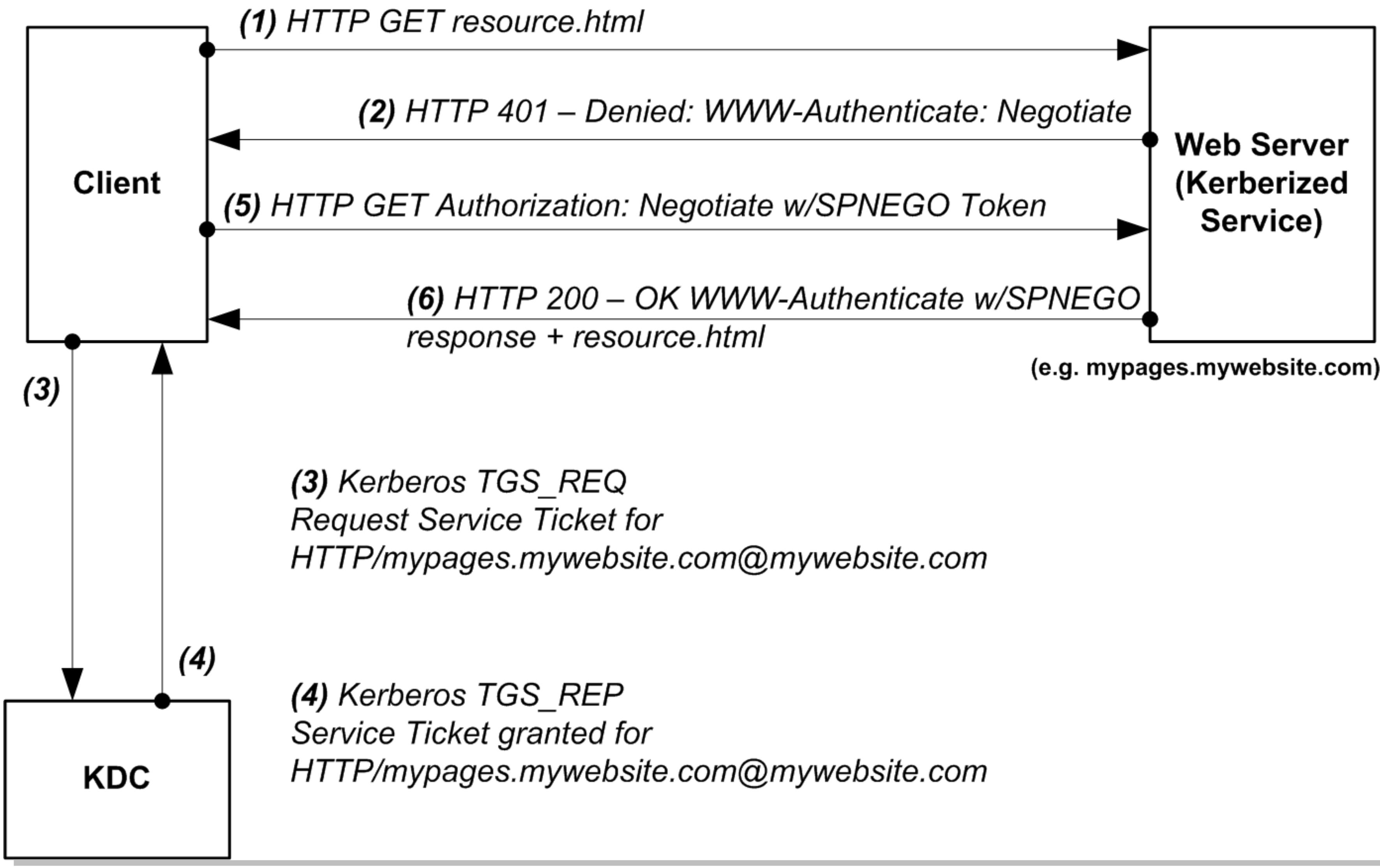
MIT Kerberos in Commercial Products

- Google
  - Enterprise Search Appliance (GSA)
- Cisco:
  - Cisco IOS - Rel. 11.2 +
  - NAC Appliance
  - ASA5000 & VPN3000 series.
- Intel:
  - VPro II Platforms (AMT)
- Red Hat:
  - Enterprise Linux & FreeIPA
- Sun/Oracle:
  - Solaris 8 to 10 and Solaris Nevada
- Yahoo
  - Hadoop infra
- Juniper:
  - Network Admission Control
- SAP R3
- NetApp:
  - Kerberized NFS
- F5 Networks:
  - BIG-IP ADC
- Other Open Source OS:
  - Ubuntu
  - Debian

MIT KIT INTERNET TRUST

BACKUP SLIDES

Kerberos in Browsers: SPNEGO



MIT KIT INTERNET TRUST