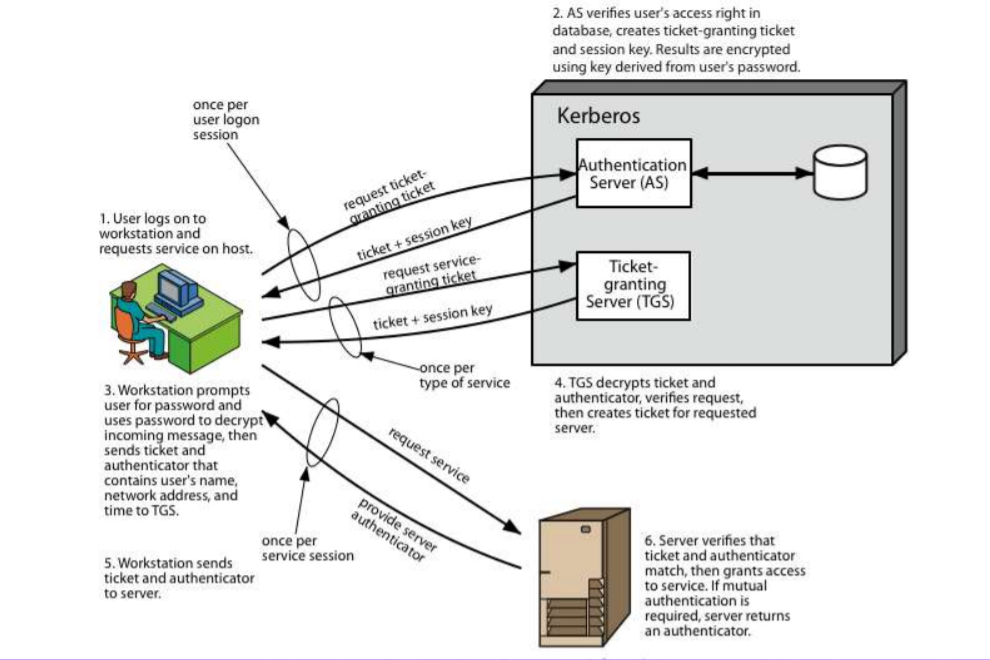
**Kerberos**

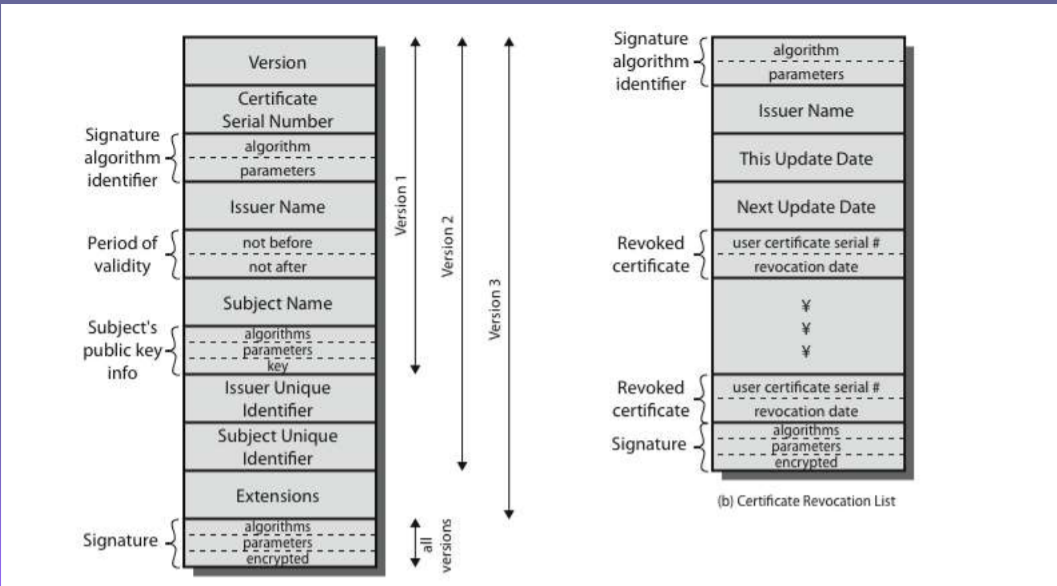
* Kerberos provides a centralized authentication server whose function is to authenticate users to servers and servers to users. In Kerberos Authentication server and database is used for client authentication. Kerberos runs as a third-party trusted server known as the Key Distribution Center (KDC). Each user and service on the network is a principal.
* The main components of Kerberos are:
  1. **Authentication Server (AS):**  
     The Authentication Server performs the initial authentication and ticket for Ticket Granting Service.
  2. **Database:**  
     The Authentication Server verifies access rights of users in database.
  3. **Ticket Granting Server (TGS):**  
     The Ticket Granting Server issues the ticket for the Server



* provides centralised private-key third-party authentication in a distributed network
* two versions in use: 4 & 5
* Its first report identified requirements as:
  + secure
  + reliable
  + transparent
  + scalable

1. obtain ticket granting ticket from AS
   1. once per session
2. obtain service granting ticket from TGT
   1. for each distinct service required
3. client/server exchange to obtain service
   1. on every service request

**X.509 CERTIFICATES**



* issued by a Certification Authority (CA), containing:
  + version (1, 2, or 3)
  + serial number (unique within CA) identifying certificate
  + signature algorithm identifier
  + issuer X.500 name (CA)
  + period of validity (from - to dates)
  + subject X.500 name (name of owner)
  + subject public-key info (algorithm, parameters, key)
  + issuer unique identifier (v2+)
  + subject unique identifier (v2+)
  + extension fields (v3)
  + signature (of hash of all fields in certificate)

**Email security**

* email is one of the most widely used and regarded network services
* currently message contents are not secure
* may be inspected either in transit
* or by suitably privileged users on destination system

**Email Security Enhancements**

* confidentiality
  + protection from disclosure
* authentication
  + of sender of message
* message integrity
  + protection from modification
* non-repudiation of origin
  + protection from denial by sender

**MIME: Multipurpose Internet Mail Extension**

* MIME is a standard which is proposed by Bell Communication in 1991 in order to expand the limited capabilities of email (Email can send messages only in NVT 7-bits ascii format).
  + Email has simple structure.
* In short, MIME is a supplementary protocol / or a add on which allows non-ascii data to be sent through email (via SMTP).
  + It allows users to exchange different kinds of data files on internet like audio, video, images, etc.
  + MIME is an extension to the internet email protocol
* Email Messages with MIME formatting are typically transmitted with standard protocols like SMTP, POP (Post Office Protocol) and IMAP (Internet Message Access Protocol).
* Although MIME was designed mainly for SMTP, its content types are also important in communication protocols.
* Ex: In http protocol for WWW, servers insert a MIME header field at the beginning of any web transmission.

**MIME Header:**

* It is added to the original e-mail header section to define transformation. There are *five headers* that we add to the original header:

1. **MIME-Version –** Defines the version of the MIME protocol. It must have the parameter *Value 1.0*, which indicates that message is formatted using MIME.
2. **Content-Type –**Type of data used in the body of the message. They are of different types like text data (plain, HTML), audio content, or video content.
3. **Content-Type Encoding –** It defines the method used for encoding the message. Like 7-bit encoding, 8-bit encoding, etc.
4. **Content Id –** It is used for uniquely identifying the message.
5. **Content description –** It defines whether the body is actually an image, video, or audio.

Why MIME? (Limitations of SMTP Protocol)

* SMTP has a very simple structure.
* SMTP can only send the messages in NVT 7-bits ascii format.
* It cannot be used for languages that don’t support 7-bits ascii format such as French, German, etc. So, in order to make SMTP more wide, we use MIME.
* It cannot be used to send binary files or video or audio data.

**S/MIME: Secure Multipurpose Internet Mail Extension**

* S/MIME is an upgrade version of MIME protocol.
* provides security for commercial emails.
* It is widely accepted method for sending digital signed and encrypted messages i.e, it allows us to digitally sign our email to verify ourselves as the legitimate sender.
* S/MIME is based on asymmetric key encryption.
* FUNCTION:
  1. Authentication
  2. Message integrity
  3. Non-repudiation
  4. Privacy
  5. Data security
* So, In short S/MIME is a protocol used to encrypt emails and digitally sign them.
* It provides two security services:

1. Digital signature (provides authentication and non-repudiation)
2. Message encryption (provides confidentiality and data-integrity)

**Pretty Good Privacy (PGP)**

* widely used de facto secure email
* developed by Phil Zimmermann
* selected best available crypto algorithms to use
* integrated into a single program
* on Unix, PC, Macintosh and other systems
* originally free, now also have commercial versions available

**PGP Operation – Authentication**

1. sender creates message
2. use SHA-1 to generate 160-bit hash of message
3. signed hash with RSA using sender's private key, and is attached to message
4. receiver uses RSA with sender's public key to decrypt and recover hash code
5. receiver verifies received message using hash of it and compares with decrypted hash code.

**PGP Operation – Confidentiality**

1. sender generates message and 128-bit random number as session key for it
2. encrypt message using CAST-128 / IDEA / 3DES in CBC mode with session key
3. session key encrypted using RSA with recipient's public key, & attached to message.
4. receiver uses RSA with private key to decrypt and recover session key
5. session key is used to decrypt message.

**PGP Operation – Confidentiality & Authentication**

* can use both services on same message
* create signature & attach to message
* encrypt both message & signature
* attach RSA/ElGamal encrypted session key

**PGP Operation – Compression**

* by default PGP compresses message after signing but before encrypting
  + so can store uncompressed message & signature for later verification
  + & because compression is non deterministic
* uses ZIP compression algorithm

**PGP Operation – Email Compatibility**

* when using PGP will have binary data to send (encrypted message etc)
* however email was designed only for text
* hence PGP must encode raw binary data into printable ASCII characters
* uses radix-64 algorithm
  + maps 3 bytes to 4 printable chars
  + also appends a CRC
  + PGP also segments messages if too big