CHƯƠNG 6: CÁC ỨNG DỤNG XÁC THỰC

6.1. Quản lý khóa

6.1.1. Phân phối khóa

Mã khóa công khai giúp giải bài toán phân phối khóa, đây là nhu cầu cấp bách cần phải tạo ra một cơ chế chia sẻ khóa trong môi trường thường xuyên trao đổi thông tin và thường xuyên thay đổi khóa. Nó bao gồm hai khía cạnh sau:

- Phân phối khóa một cách công khai nhưng đảm bảo được bí mật.
- Sử dụng mã khóa công khai để phân phối khóa mật (còn khóa mật dùng để mã hoá thông tin).

  Để phân phối khóa công khai có thể xem xét sử dụng một trong những giải pháp sau:
  - Thông báo công khai khóa của người sử dụng.
  - Thư mục truy cập công cộng cho mọi người.
  - Chủ quyền khóa công khai, người nắm giữ khóa công khai.
  - Chứng nhận khóa công khai, khóa công khai của người sử dụng được nơi có thẩm quyền chứng nhận.

Thông báo công khai

- Người dùng phân phối khóa công khai cho người nhận hoặc thông báo rộng rãi cho cộng đồng. Chẳng hạn như người sử dụng có thể tự bổ sung khóa PGP vào thư điện tử hoặc gửi cho nhóm chia sẻ tin hoặc một danh sách thư điện tử.
- Điểm yếu chính của thông báo công khai là mạo danh: một người nào đó có thể tạo khóa và tuyên bố mình là một người khác và gửi thông báo cho mọi người khác. Cho đến khi giả mạo bị phát hiện thì kẻ mạo danh đã có thể lừa trong vai trò người khác.

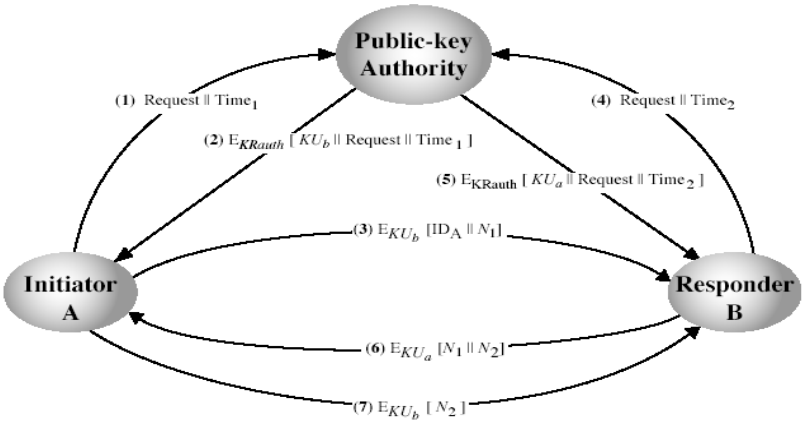
Thư mục truy cập công cộng

- Dùng thư mục truy cập công cộng có thể đạt được tính an toàn cao hơn bằng cách đăng ký khóa với thư mục công cộng để đăng tải và chia sẻ cho mọi người.
- Thư mục cần được đảm bảo tin cậy với các tính chất sau:
  - Chứa việc nhập tên và khóa công khai.
  - Người dùng đăng ký mật với Thư mục.
  - Người dùng có thể thay khóa bất cứ lúc nào.
  - Thư mục được in định kỳ.
  - Thư mục có thể truy cập qua mạng.
- Mô hình trên vẫn còn có các lỗ hổng để kẻ xâm nhập sửa hoặc giả mạo khi vào hệ thống.

Chủ quyền khóa công khai

Đây là bước cải thiện tính an toàn bằng kiểm soát chặt chẽ tập trung việc phân phối khóa từ Thư mục. Nó bao gồm các tính chất của một Thư mục như đã nêu ở phần

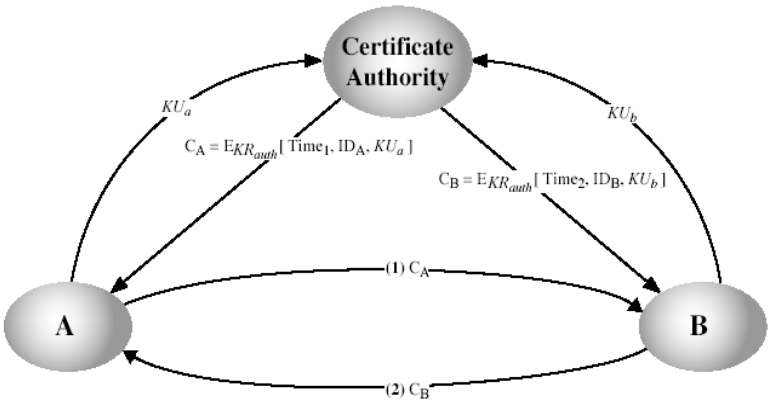
trước và đòi hỏi người dùng biết khóa công khai của Thư mục đó. Sau đó người dùng nhận được bất kỳ khóa công khai mong muốn nào một cách an toàn, bằng cách truy cập thời gian thực đến Thư mục khi cần đến khóa. Tuy nhiên yêu cầu truy cập thời gian thực là một nhược điểm của cách phân phối khóa này. Cụ thể trong kịch bản sau hai người sử dụng chia sẻ khóa công khai của mình cho nhau thông qua việc sử dụng khóa công khai của Chủ quyền để nhận được khóa công khai của đối tác và trao đổi qua lại để khẳng định người này đã biết thông tin của người kia.



Chứng nhận khóa công khai

Chứng nhận cho phép trao đổi khóa không cần truy cập thời gian thực đến Chủ quyền thư mục khóa công khai. Để làm việc đó cần chứng nhận trói danh tính của người sử dụng với khóa công khai của anh ta và "đóng dấu vào giấy chứng nhận" đó để tránh giả mạo. Các thông tin đi kèm thông thường là chu kỳ kiểm định, quyền sử dụng, thời hạn,…

Nội dung trên được ký bởi khóa riêng tin cậy của Chủ quyền chứng nhận (CA, Certificate Authority). Do khóa công khai của CA được thông báo rộng rãi, nên chứng nhận đó có thể được kiểm chứng bởi một người nào đó biết khóa công khai của Chủ quyền chứng nhận.



6.1.2. Phân phối công khai các khóa mật

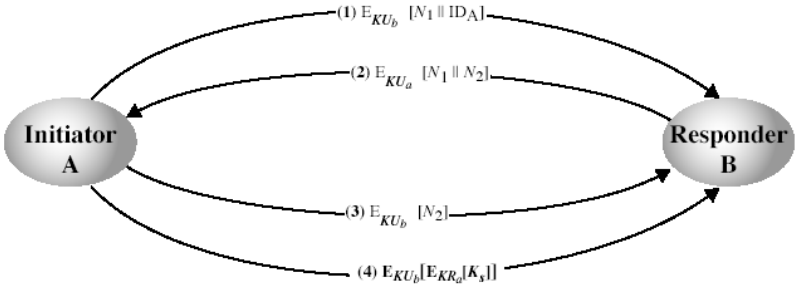
Nói chung có thể sử dụng các phương pháp trên để nhận được khóa công khai của người định trao đổi thông tin. Khóa công khai đó dùng cho mục đích mã hoá, giải mã

hoặc xác nhận thông tin là của đối tác. Nhưng các thuật toán khóa công khai chậm, nên giá để bảo mật thông tin là đắt. Do đó thông thường dùng khóa đối xứng để mã hoá và giải mã nội dung bản tin. Khóa đó còn được gọi là khóa phiên hay khóa kỳ (Section Key). Có một số cách thỏa thuận khóa phiên phù hợp giữa hai người sử dụng.

Phân phối khóa mật đơn giản

- Phân phối khóa mật đơn giản được đề xuất bởi Merkle vào năm 1979:
  - A tạo ra một cặp khóa công khai mới tạm thời.
  - A gửi B một khóa công khai và danh tính của họ.
  - B tạo ra khóa phiên và gửi nó cho A sử dụng khóa công khai được cung cấp.
  - A giải mã khóa phiên và cả hai cùng dùng nó.
- Vấn đề nằm ở chỗ, kẻ thù có thể ngăn hoặc đóng giả cả hai bên của thủ tục.

Nếu có khóa công khai, thì khóa phiên được trao đổi an toàn.



6.1.3. Trao đổi khóa bằng phương pháp kết hợp:

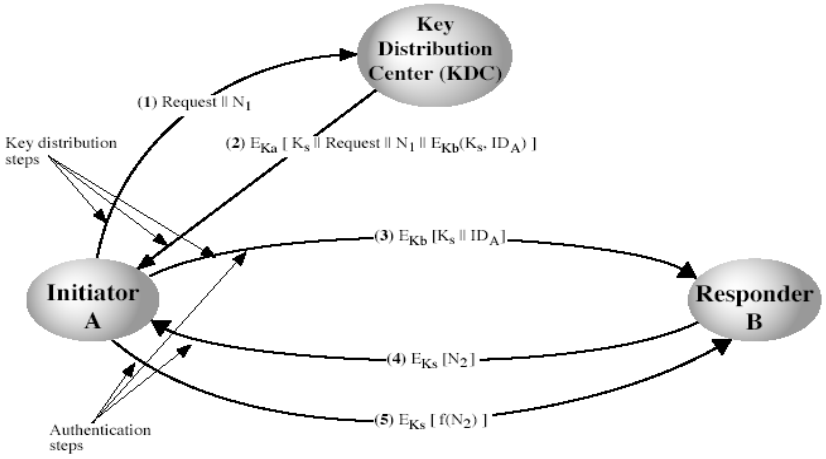
Ta có thể kết hợp sử dụng Trung tâm phân phối khóa để phân phối khóa phiên như trên mô hình máy chủ của IBM. Trung tâm chia sẻ khóa chính (master key) với mỗi người sử dụng và phân phối khóa phiên sử dụng khóa chính với Trung tâm. Sơ đồ khóa công khai được dùng để phân phối khóa chính. Sơ đồ ba lớp này đặc biệt hữu ích khi người sử dụng phân tán rộng. Các yêu cầu căn bản của hệ thống là chất lượng thực hiện và sự tương thích nền tảng.

Phân phối khóa dùng chung

Sơ đồ đối xứng đòi hỏi cả hai đối tác chia sẻ khóa bí mật chung. Vấn đề đặt ra là phân phối khóa mật này như thế nào. Thông thường các hệ mật thường bị sập vì bị bẻ khóa trong sơ đồ phân phối khóa.

Đối với hai đối tác A và B cho trước có một số cách phân phối khóa khác nhau:

1. A lựa chọn khóa và truyền tay cho B.
2. Đối tác thứ ba có thể chọn khóa và phân phối cho A và B.
3. A và B trao đổi trước có thể dùng khóa trước để mã khóa mới.
4. A và B trao đổi mật với đối tác thứ 3 là C, C chuyển tiếp giữa A và B.



Kịch bản phân phối khóa

Phân loại khóa

Thông thường khóa phân loại như sau:

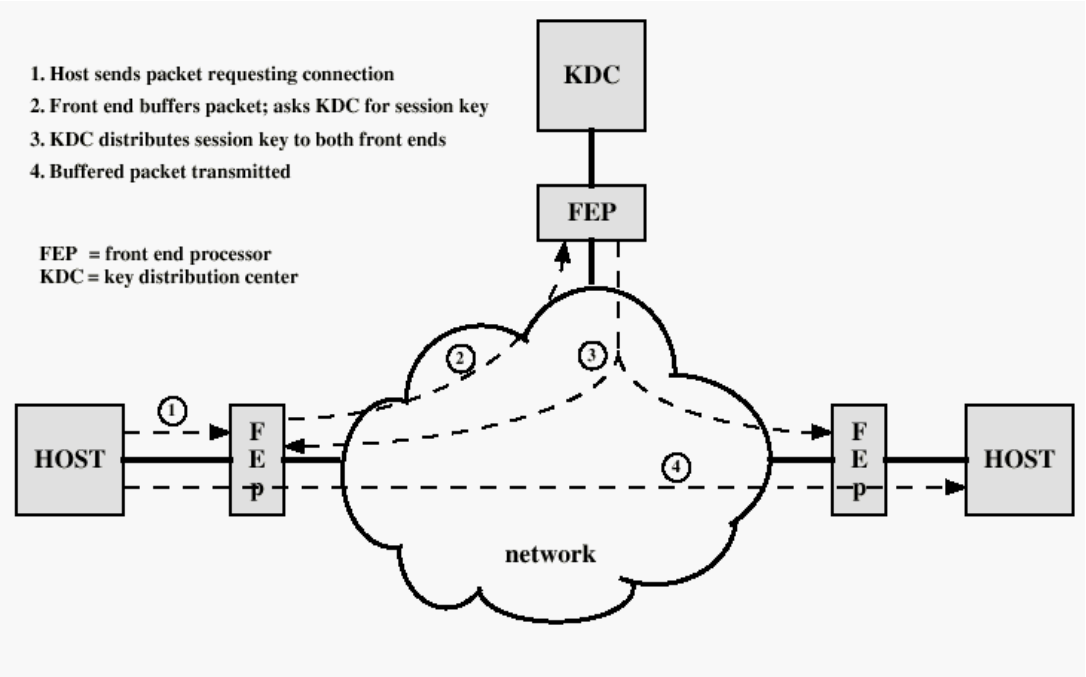
- Khóa phiên (Section Key):
  - Khóa tạm thời.
  - Dùng để mã hoá dữ liệu giữa nhóm người sử dụng.
  - Sử dụng cho một phiên logic và sau đó bỏ đi.
- Khóa chính (Master Key):
  - Dùng để mã các khóa phiên.
  - Chia sẻ giữa người sử dụng và trung tâm phân phối khóa.

Vấn đề phân phối khóa

Đối với mạng lớn đòi hỏi phân cấp Trung tâm phân phối khóa KDC, nhưng cần phải tạo tin cậy cho nhau, giữa người sử dụng với Trung tâm và các Trung tâm với nhau. Thời gian sống của khóa bộ phận cần được hạn chế để cho an toàn hơn. Sử dụng phân phối khóa tự động thay mặt người dùng, nhưng phải có hệ thống tin cậy, các khóa cấp phát được sinh ra càng ngẫu nhiên càng tốt. Cần phải có hệ thống phân phối khóa phân tán và phân cấp. Đồng thời cần hỗ trợ kiểm soát mục đích sử dụng khóa.

Tự động phân phối khóa cho giao thức hướng kết nối

- Máy chủ gửi gói yêu cầu kết nối.
- Bộ xử lý đầu cuối FEP lưu gói và đề nghị KDC cấp khóa phiên.
- KDC cấp và mã khóa phiên gửi cho hai bộ xử lý đầu cuối của người nhận và người gửi.
- Gói lưu được mã hoá bằng khóa phiên và gửi trên mạng



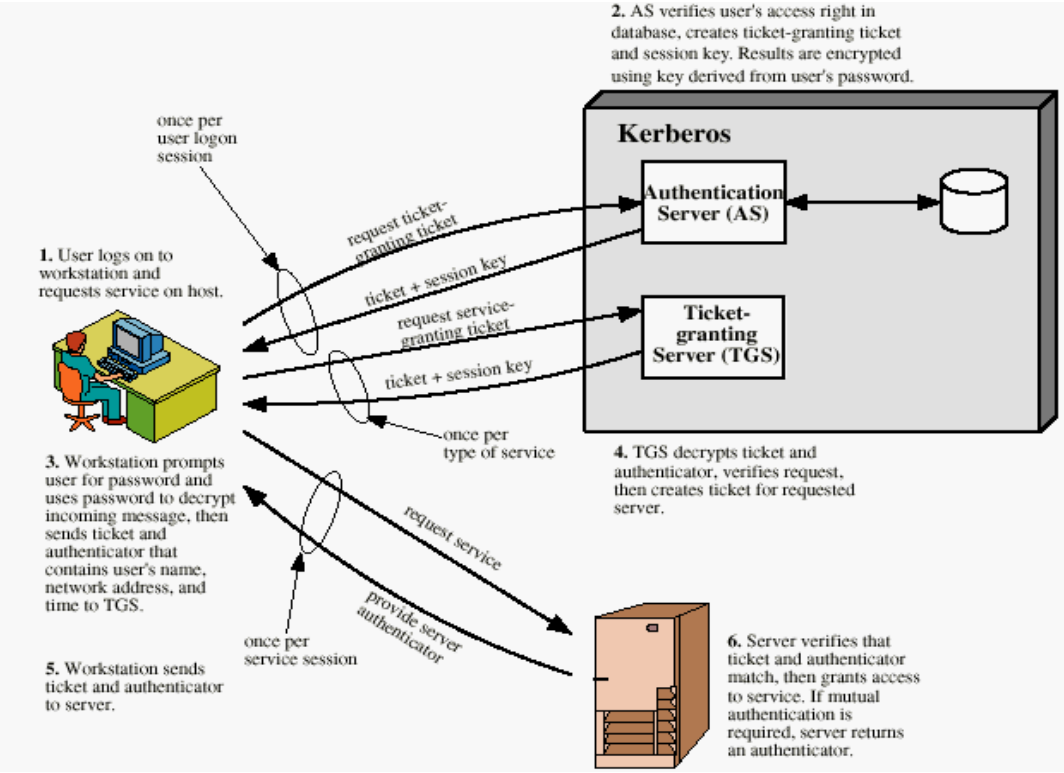
6.2. Kerberos

Đây là mô hình Hệ thống khóa máy chủ tin cậy của MIT (Trường Đại học Kỹ thuật Massachusetts) để cung cấp xác thực có bên thứ ba dùng khóa riêng và tập trung. Cho phép người sử dụng truy cập vào các dịch vụ phân tán trong mạng. Tuy nhiên không cần thiết phải tin cậy mọi máy trạm, thay vì đó chỉ cần tin cậy máy chủ xác thực trung tâm. Đã có hai phiên bản đang sử dụng là: Kerberos 4 và Kerberos 5.

6.2.1. Các yêu cầu của Kerrberos

Trên môi trường phân tán, người sử dụng tại các máy trạm muốn truy cập đến các dịch vụ trên các máy chủ phân tán. Chúng ta muốn các máy chủ hạn chế truy cập và có khả năng xác thực các yêu cầu dịch vụ. Yêu cầu đối với hệ thống Kerberos là

- An toàn.
- Tin cậy.
- Trong suốt
- Có thể mở rộng.



6.2.2. Tổng quan Kerberos 4

Là sơ đồ xác thực dùng bên thứ ba và có máy chủ xác thực (AS – Authentication Server). Người dùng thỏa thuận với AS về danh tính của mình, AS cung cấp sự tin cậy xác thực thông qua thẻ cấp thẻ TGT (Ticket Granting Ticket). Người sử dụng thường xuyên yêu cầu TGS cho truy cập đến các dịch vụ khác dựa trên thẻ cấp thẻ TGT của người sử dụng và máy chủ cung cấp thẻ (TGS – Ticket Granting Server) cung cấp các thẻ dịch vụ theo yêu cầu và thẩm quyền.

6.2.3. Trao đổi Kerberos 4

Người sử dụng nhận thẻ được cấp từ máy chủ xác thực AS, mỗi thẻ cho một phiên làm việc và cũng nhận thẻ cấp dùng dịch vụ (Service Granting Ticket) từ TGT. Mỗi thẻ dùng cho một dịch vụ khác nhau được yêu cầu, thông qua việc trao đổi giữa máy chủ/trạm để nhận được dịch vụ.

6.2.4. Các lãnh địa Kerberos

Môi trường Kerberos bao gồm: máy chủ Kerberos, một số máy trạm đã được đăng ký với máy chủ, các máy chủ ứng dụng chia sẻ khóa với máy chủ. Một hệ thống như vậy được gọi là một lãnh địa Kerberos. Thông thường là một miền hành chính duy nhất. Nếu có nhiều lãnh địa thì các máy chủ Kerberos cần phải chia sẻ khóa và tin cậy nhau.

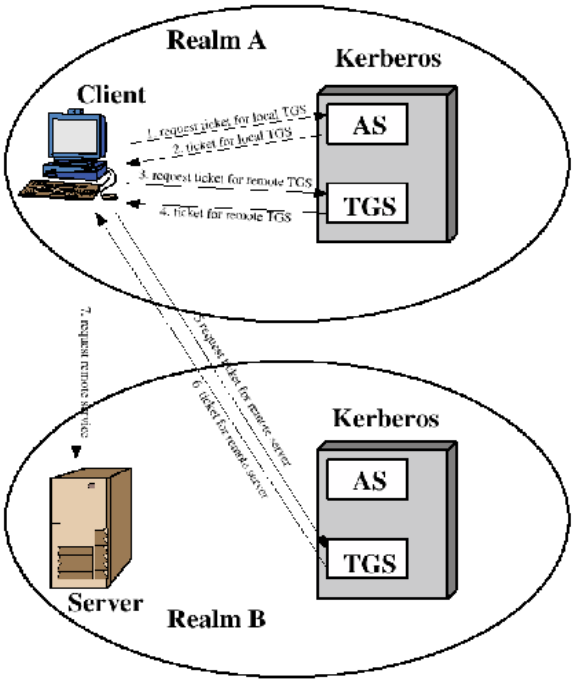


Figure 4.2 Request for Service in Another Realm

6.2.5. Kerberos phiên bản 5

Kerberos 5 được phát triển vào giữa những năm 1990, được thiết kế theo chuẩn RFC. Nó cung cấp những cải tiến so với phiên bản 4, cụ thể hướng tới các thiếu xót về môi trường, thuật toán mã, thủ tục mạng, thứ tự byte thông điệp, thời gian sử dụng thẻ, truyền tiếp xác thực, xác thực lãnh địa con và các sự khác biệt về kỹ thuật như: mã kép dùng mã hai lần thẻ bằng khóa mật của máy chủ đích và khóa riêng của người sử dụng, khắc phục các dạng sử dụng không chuẩn trong phiên bản trước, khóa phiên được mã bằng khóa xác thực của TGS cộng thêm với yếu tố thời gian của lần sử dụng, chống tấn công mật khẩu.

Sau đây ta xem xét chi tiết mô hình Kerberos

Kerberos là một giao thức x ác thực mạng, nó cho phép các cá nhân giao tiếp với nhau trên một mạng không an toàn bằng cách xác thực người dùng này với người dùng khác theo một cơ chế bảo mật và an toàn . Kerberos ngăn chặn việc nghe trộm thông tin cũng như tấn công thay thế và đảm bảo tính toàn vẹn của dữ liệu . Kerberos hoạt động theo mô hình máy trạm /máy chủ và nó thực hiện quá trình x ác thực 2 chiều - cả người dùng và dịch vụ xác thực lẫ n nhau. Kerberos được xây dựng dựa trên mô hình mã hóa khóa đối xứng và đòi hỏi một thành phần thứ ba tin cậy tham gia vào quá trình xác thực.

1) Mô tả giao thức

Kerberos sử dụng một đối tác tin cậy thứ ba để thực hiện quá trình xác thực được gọi là Trung tâm phân phối khóa bao gồm 2 phần riêng biệt: một máy chủ xác thực (AS) và một máy chủ cấp thẻ (TGS). Kerberos làm việc dựa trên các thẻ để thực hiện quá trình xác thực người dùng.

Kerberos duy trì một cơ sở dữ liệu chứa các khóa bí mật. Mỗi thực thể trên mạng (máy trạm hoặc máy chủ) đều chia sẻ một khóa bí mật giữa bản thân nó với Kerberos. Để thực hiện quá trình giao tiếp giữa hai thực thể, Kerberos tạo ra một khóa phiên. Khóa này dùng để bảo mật quá trình tương tác giữa các thực thể với nhau.

2) Hoạt động của Kerberos

Quá trình hoạt động của giao thức (AS = Máy chủ xác thực, TGS = Máy chủ cấp thẻ, C = Máy trạm, S = Dịch vụ):

- Người dùng nhập vào tên truy cập và mật khẩu ở phía máy trạm.
- Máy trạm thực hiện thuật toán băm một chiều trên mật khẩu được nhập vào và biến nó trở thành khóa bí mật của người dùng.
- Máy trạm gửi một thông điệp dưới dạng bản rõ đến AS để yêu cầu dịch vụ. Không có khóa bí mật cũng như mật khẩu nào được gởi đến AS.
- AS kiểm tra xem có tồn tại người dùng C trong cơ sở dữ liệu của nó hay không. Nếu có, nó gửi ngược lại cho máy trạm hai thông điệp:
  - Thông điệp A: chứa khóa phiên Máy trạm/TGS được mã hóa bởi khóa bí mật của người dùng.
  - Thông điệp B: chứa Thẻ (bao gồm ID của máy trạm, địa chỉ mạng của máy trạm, kỳ hạn thẻ có giá trị và một khóa phiên máy trạm/TGS) được mã hóa sử dụng khóa bí mật của TGS.
- Khi máy trạm nhận được thông điệp A và B, nó giải mã thông điệp A để lấy khóa phiên máy trạm/TGS. Khóa phiên này được sử dụng cho quá trình tra ao đổi tiếp theo với TGS. Ở đây máy trạm không thể giải mã thông điệp B bởi vì nó được mã hóa bởi khóa bí mật của TGS.
- Khi yêu cầu dịch vụ (S), máy trạm gửi hai thông điệp sau đến TGS:
  - Thông điệp C: Gồm thông điệp B và ID của dịch vụ được yêu cầu
  - Thông điệp D: chứa Authenticator (gồm ID máy trạm và nhãn thời gian - timestamp) được mã hóa bởi khóa phiên máy trạm/TGS.
- Khi nhận được thông điệp C và D, TGS giải mã thông điệp D sử dụng khóa phiên máy trạm/TGS và gửi hai thông điệp ngược lại cho máy trạm:
  - Thông điệp E: chứa thẻ (máy trạm đến máy chủ) (bao gồm ID máy trạm, địa chỉ mạng của máy trạm, kỳ hạn thẻ có giá trị và một khóa phiên máy trạm/dịch vụ) được mã hóa bởi khóa bí mật của dịch vụ.
  - Thông điệp F: chứa khóa phiên của máy trạm /máy chủ được mã hóa bởi khóa phiên máy trạm/TGS.
- Khi nhận được thông điệp E và F, máy trạm sau đó gởi một Authenticator mới và một thẻ (máy trạm đến máy chủ) đến máy chủ chứa dịch vụ được yêu cầu.
  - Thông điệp G: chứa thẻ (máy trạm đến máy chủ) được mã hóa sử dụng khóa bí mật của máy chủ.
  - Thông điệp H: một Authenticator mới chứa ID máy trạm, Timestamp và được mã hóa sử dụng khóa phiên máy trạm/máy chủ.

- Sau đó, máy chủ giải mã thẻ sử dụng khóa bí mật của chính nó và gửi một thông điệp cho máy trạm để xác nhận tính hợp lệ thực sự của máy trạm và sự sẵn sàng cung cấp dịch vụ cho máy trạm.
  - Thông điệp I: chứa giá trị Timestamp trong Authenticator được gửi bởi máy trạm sẽ được cộng thêm 1, được mã hóa bởi khóa phiên máy trạm/máy chủ.
- Máy trạm sẽ giải mã sự xác nhận này sử dụng khóa chia sẻ giữa nó với máy chủ, và kiểm tra xem giá trị timestamp có được cập nhật đúng hay không. Nếu đúng, máy trạm có thể tin tưởng máy chủ và bắt đầu đưa ra các yêu cầu dịch vụ gửi đến máy chủ.
- Máy chủ cung cấp dịch vụ được yêu cầu đến máy trạm.

3) Hạn chế của Kerberos

Kerberos thích hợp cho việc cung cấp các dịch vụ xác thực, phân quyền và bảo đảm tính mật của thông tin trao đổi trong phạm vi một mạng hay một tập hợp nhỏ các mạng. Tuy nhiên, nó không thật thích hợp cho một số chức năng khác, chẳng hạn như ký điện tử (yêu cầu đáp ứng cả hai nhu cầu xác thực và bảo đảm không chối cãi được). Một trong những giả thiết quan trọng của giao thức Kerberos là các máy chủ trên mạng cần phải tin cậy được. Ngoài ra, nếu người dùng chọn những mật khẩu dễ đoán thì hệ thống dễ bị mất an toàn trước kiểu tấn công từ điển, tức là kẻ tấn công sẽ sử dụng phương thức đơn giản là thử nhiều mật khẩu khác nhau cho đến khi tìm được giá trị đúng.

Do hệ thống hoàn toàn dựa trên mật khẩu để xác thực người dùng, nếu bản thân các mật khẩu bị đánh cắp thì khả năng tấn công hệ thống là không có giới hạn. Điều này dẫn đến một yêu cầu rất căn bản là Trung tâm phân phối khóa cần được bảo vệ nghiêm ngặt. Nếu không thì toàn bộ hệ thống sẽ trở nên mất an toàn.

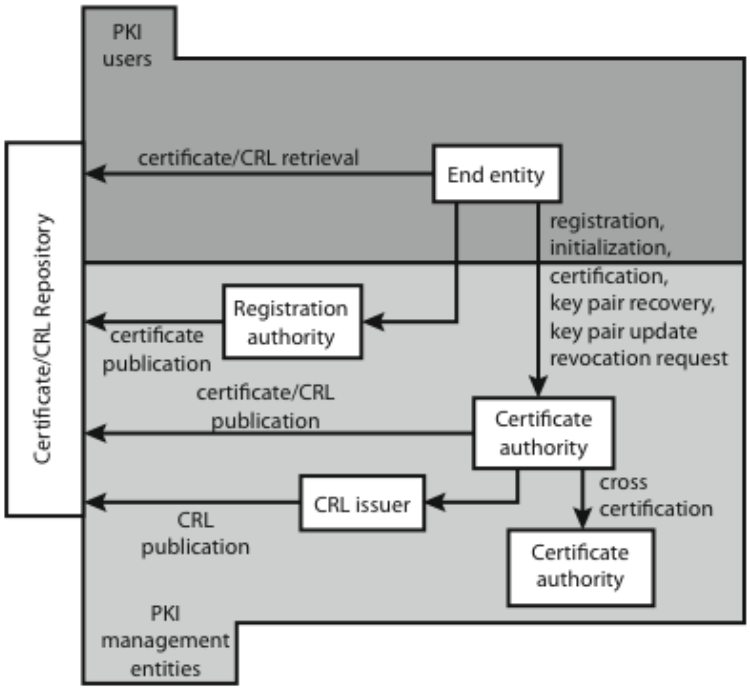
Toàn vẹn dữ liệu

Đối với mỗi hệ bảo mật toàn vẹn dữ liệu là một yêu cầu không thể thiếu, để đảm bảo tính toàn vẹn dữ liệu thực sự, các thuật mã hoá như mã hoá băm, mã xác nhận thông điệp (MAC) và chữ ký điện tử có thể cùng được triển khai đồng loạt. Về cơ bản, những biện pháp này sử dụng các hàm một chiều, nghĩa là dữ liệu không thể bị giải mã ngay cả khi đã biết khóa để mã hoá nó.

6.3. Cơ sở hạ tầng Khóa công khai PKI

Nhiệm vụ của PKI:

- Quản lý danh tính người sử dụng với khóa công khai của người đó.
- Cấp chứng nhận của Chủ quyền Giấy chứng nhận CA cho người sử dụng.
- Huỷ và Thu hồi các giấy chứng nhận không còn hiệu lực.
- Tạo ra các Thư mục để lưu trữ các chứng nhận và danh sách thu hồi (CRL).
- Cung cấp dịch vụ sẵn sàng cung cấp cho người sử dụng như: đăng ký, truy cập, xin giấy chứng nhận, đưa ra danh sách thu hồi CRL.



6.4. An toàn thư điện tử

Thư điện tử là một trong những dịch vụ mạng được coi trọng và ứng dụng rộng rãi nhất. Tuy nhiên nội dung của các mẩu tin có thể bị quan sát trên đường truyền hoặc bởi những người có thẩm quyền thích hợp ở hệ thống đầu cuối.

Nâng cao an toàn thư điện tử là mục đích quan trọng của mọi hệ thống trao đổi thư. Ở đây phải đảm bảo các yêu cầu sau: tính bảo mật nội dung tin gửi, xác thực người gửi mẩu tin, tính toàn vẹn của mẩu tin, hơn nữa bảo vệ khỏi bị sửa, tính chống từ chối gốc, chống từ chối của người nhận.

6.4.1. Dịch vụ PGP

PGP (Pretty Good Privacy) là một dịch vụ về bảo mật và xác thực được sử dụng rộng rãi cho chuẩn an toàn thư điện tử. PGP được phát triển bởi Phil Zimmermann. Ở đây lựa chọn các thuật toán mã hoá tốt nhất để dùng, tích hợp thành một chương trình thống nhất, có thể chạy trên Unix, PC, Macintosh và các hệ thống khác. Ban đầu là miễn phí, bây giờ có các phiên bản thương mại. Sau đây chúng ta xem xét hoạt động của PGP

Thao tác PGP – xác thực

Người gửi tạo mẩu tin, sử dụng SHA-1 để sinh Hash 160 bit của mẩu tin, ký hash với RSA sử dụng khóa riêng của người gửi và đính kèm vào mẩu tin.

Người nhận sử dụng RSA với khóa công khai của người gửi để giải mã và khôi phục bản hash. Người nhận kiểm tra mẩu tin nhận sử dụng bản hash của nó và so sánh với bản hash đã được giải mã.

Thao tác PGP – bảo mật

Người gửi tạo mẩu tin và số ngẫu nhiên 128 bit như khóa phiên cho nó, mã hoá mẩu tin sử dụng CAST-128/IDEA/3DES trong chế độ CBC với khóa phiên đó. Khóa phiên được mã sử dụng RSA với khóa công khai người nhận và đính kèm với mẩu tin.

Người nhận sử dụng RSA với khóa riêng để giải mã và khôi phục khóa phiên. Khóa phiên được sử dụng để giải mã mẩu tin.

Thao tác PGP - Bảo mật và xác thực

Có thể sử dụng cả hai dịch vụ trên cùng một mẩu tin. Tạo chữ ký và đính vào mẩu tin, sau đó mã cả mẩu tin và chữ ký. Đính khóa phiên đã được mã hoá RSA/ElGamal.

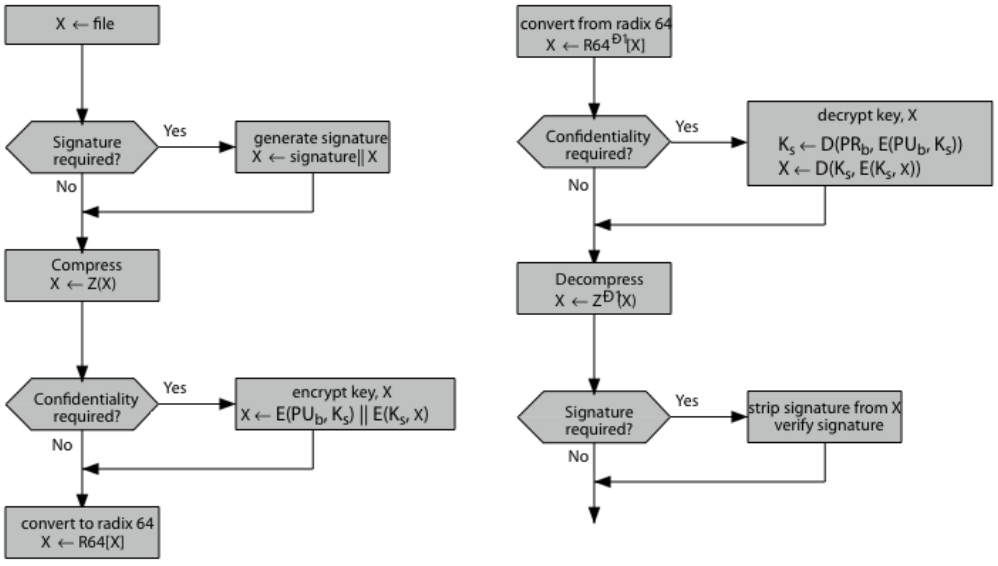
Thao tác PGP – nén

Theo mặc định PGP nén mẩu tin sau khi ký nhưng trước khi mã. Như vậy cần lưu mẩu tin chưa nén và chữ ký để kiểm chứng về sau. Vì rằng nén là không duy nhất. Ở đây sử dụng thuật toán nén ZIP.

Thao tác PGP – tương thích thư điện tử

Khi sử dụng PGP sẽ có dữ liệu nhị phân để gửi (mẩu tin được mã). Tuy nhiên thư điện tử có thể thiết kế chỉ cho văn bản. Vì vậy PGP cần mã dữ liệu nhị phân thô vào các ký tự ASCII in được. Sau đó sử dụng thuật toán Radix 64, ánh xạ 3 byte vào 4 ký tự in được và bổ sung kiểm tra thừa quay vòng CRC để phát hiện lỗi khi truyền. PGP sẽ chia đoạn mẩu tin nếu nó quá lớn.

Tóm lại, cần có khóa phiên cho mỗi mẩu tin có kích thước khác nhau: 56 bit – DES, 128 bit CAST hoặc IDEA, 168 bit Triple – DES, được sinh ra sử dụng dữ liệu đầu vào ngẫu nhiên lấy từ sử dụng trước và thời gian gõ bàn phím của người sử dụng.

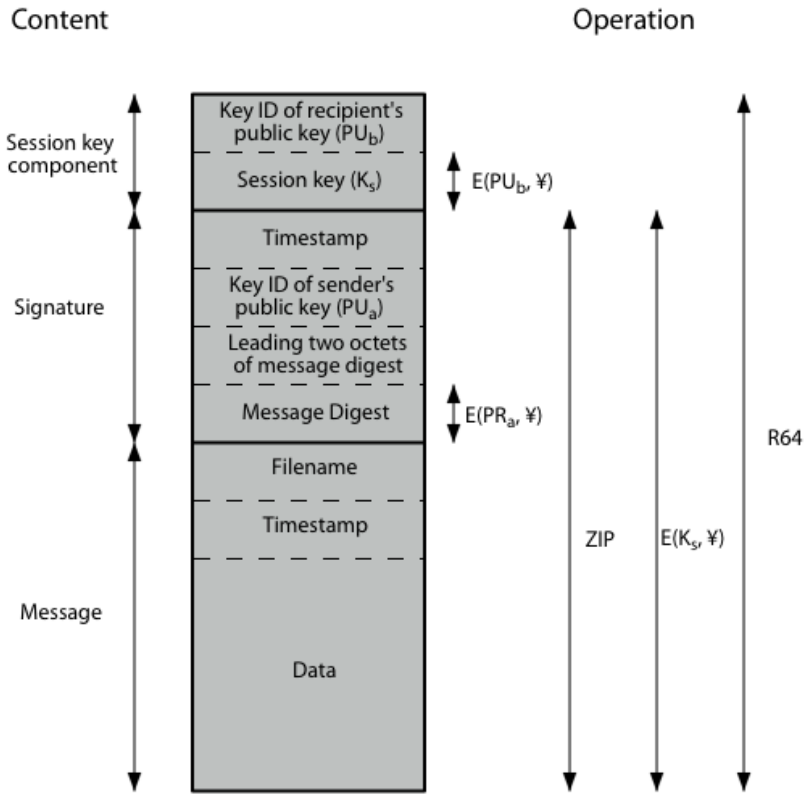


(a) Generic Transmission Diagram (from A) (b) Generic Reception Diagram (to B)

6.4.2. Khóa riêng và công khai của PGP

Vì có nhiều khóa riêng và khóa công khai có thể được sử dụng nên cần phải xác định rõ cái nào được dùng để mã khóa phiên trong mẩu tin. Có thể gửi khóa công khai đầy đủ với từng mẩu tin. Nhưng điều đó là không đủ vì cần phải nêu rõ danh tính của người

gửi. Do đó có thể sử dụng định danh khóa để xác định người gửi. Có ít nhất 64 bit có ý nghĩa của khóa và là duy nhất, có thể sử dụng định danh của khóa trong chữ ký.



Định dạng thông điệp PGP

Các chùm khóa PGP

Mỗi người sử dụng PGP có một cặp chùm khóa. Chùm khóa công khai chứa mọi khóa công khai của những người sử dụng PGP khác được người đó biết và được đánh số bằng định danh khóa (ID key). Chùm khóa riêng chứa các cặp khóa công khai/riêng của người đó được đánh số bởi định danh khóa và mã của khóa lấy từ giai đoạn duyệt bản băm hash. An toàn của khóa công khai như vậy phụ thuộc vào độ an toàn của giai đoạn duyệt.

Private Key Ring

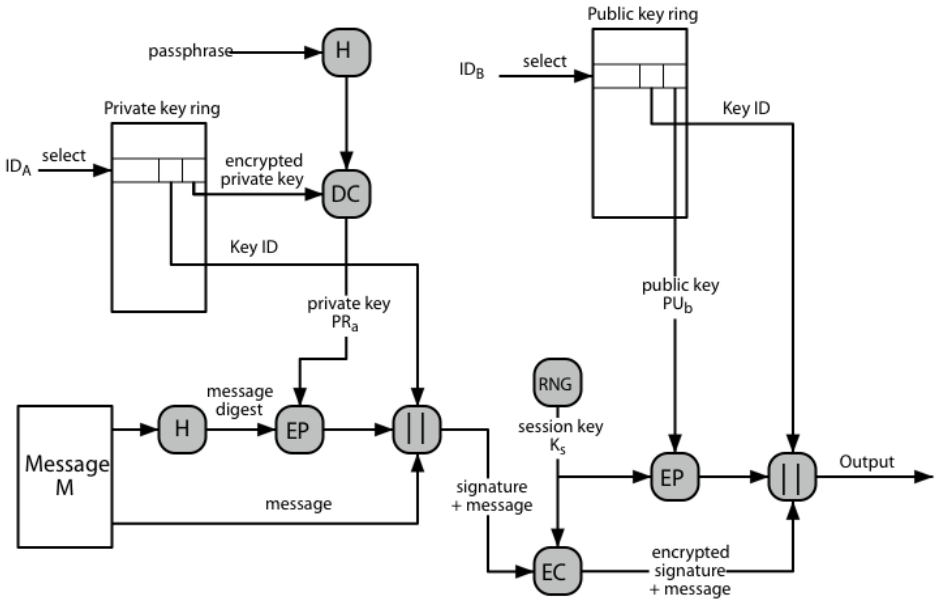
Timestamp	Key ID*	Public Key	Enerypted Private Key	User ID*
•	•	•	•	•
•	•	•	•	•
•	•	•	•	•
T_1	$KU_i \bmod 2^{64}$	KU_1	$E_{H(P1)}[KR_1]$	User 1
•	•	•	•	•
•	•	•	•	•
•	•	•	•	•

Public Key Ring

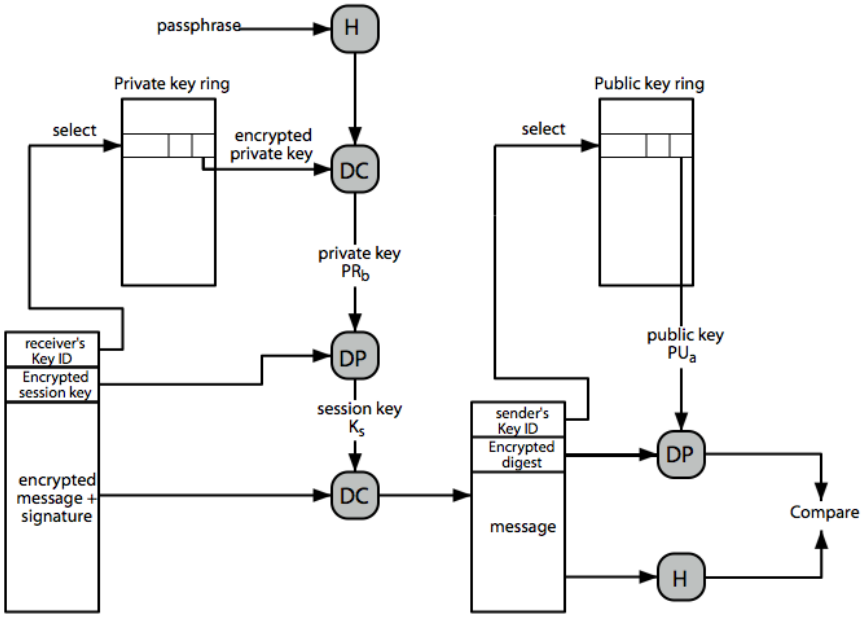
Timestamp	Key ID*	Public Key	Owner Trust	User ID*	Key Legitimacy	Signature (s)	Signature Trust (s)
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•
T_1	$KU_i \bmod 2^{64}$	KU_1	Trust_flagi	User i	Trust_flagi		
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•
•	•	•	•	•	•	•	•

Sinh mẩu tin PGP

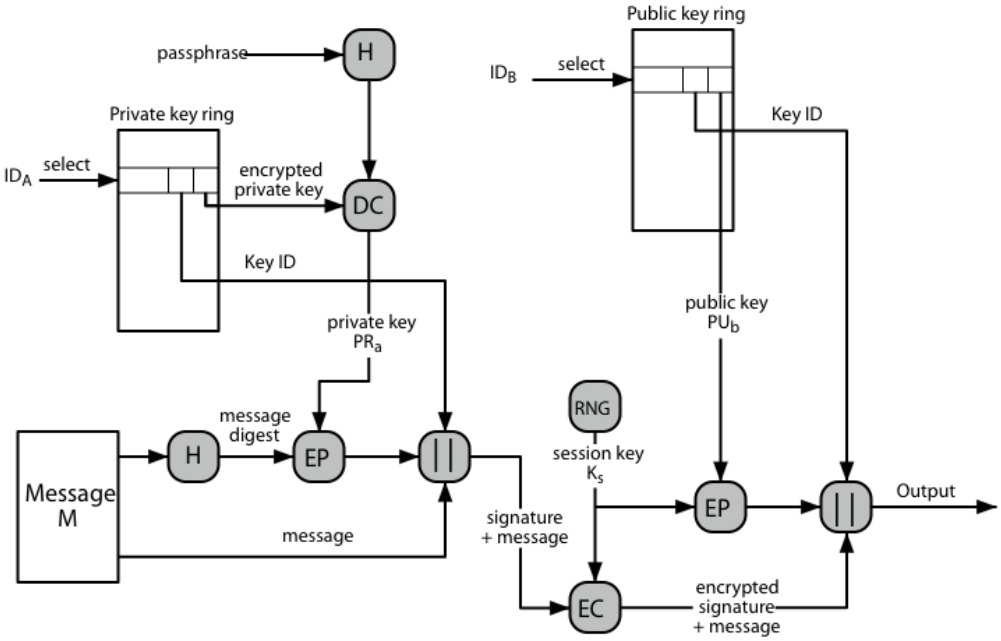
Sơ đồ sau mô tả quy trình sinh mẩu tin PGP để gửi cho người nhận.



Nhận mẩu tin PGP



Sơ đồ sau nêu cách người nhận giải mã, kiểm chứng thông tin để đọc mẩu tin.



6.4.3. Quản lý khóa PGP

Tốt hơn hết là dựa vào chủ quyền chứng nhận. Trong PGP mỗi người sử dụng có một CA của mình. Có thể ký khóa cho người sử dụng mà anh ta biết trực tiếp. Tạo thành "Web của niềm tin", cần tin cậy khóa đã được ký và tin cậy các khóa mà các người khác ký khi dùng một dây chuyền các chữ ký đến nó.

Chùm khóa chứa cả các chỉ dẫn tin cậy. Người sử dụng có thể thu hồi khóa của họ.

6.5. Dịch vụ xác thực X.509

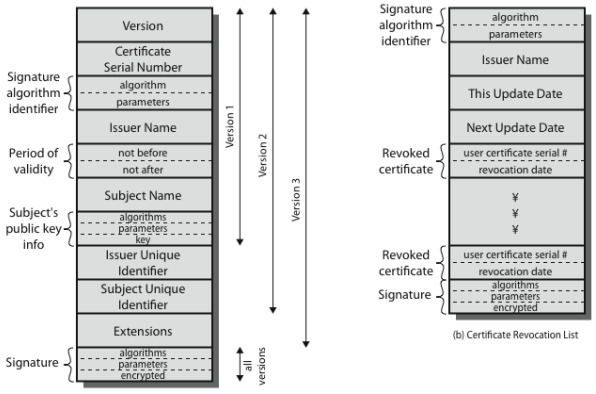
Dịch vụ xác thực X.509 là một phần của chuẩn dịch vụ thư mục X.500. Ở đây các máy chủ phân tán bảo trì cơ sở dữ liệu thông tin của người sử dụng và xác định khung cho các dịch vụ xác thực. Thư mục chứa các chứng nhận khoá công khai, khoá công khai của người sử dụng được ký bởi chủ quyền chứng nhận. Để thống nhất dịch vụ cũng xác định các thủ tục xác thực, sử dụng mã khoá công khai và chữ ký điện tử. Tuy thuật toán không chuẩn nhưng được RSA đề xuất. Các chứng nhận X.509 được sử dụng rộng rãi.

6.5.1. Các chứng nhận X.509

Được phát hành bởi Chủ quyền chứng nhận (Certification Authority – CA) bao gồm:

- Các phiên bản 1,2 hoặc 3.
- Số sổ (duy nhất với CA) xác định chứng nhận.
- Thuật toán xác định chữ ký.
- Xuất bản tên X.500 (CA).
- Chu kỳ hiệu lực (từ-đến ngày).
- Đối tượng của tên X.500 (tên của người sở hữu).
- Đối tượng thông tin khoá công khai (thuật toán, các tham số, khoá)
- Định danh duy nhất xuất bản (phiên bản 2+).
- Định danh duy nhất đối tượng (phiên bản 2+).
- Các trường mở rộng (phiên bản 3).
- Chữ ký (hoặc hash của các trường trong chứng nhận).

Ký hiệu CA<<A>> là chứng nhận cho A được ký bởi CA.



6.5.2. Nhận chứng nhận

Người sử dụng bất kỳ có thể trao đổi với CA để nhận được chứng nhận. Chỉ CA có thể sửa chứng nhận. Vì không thể bị giả mạo nên chứng nhận có thể được đặt trong thư mục công cộng.

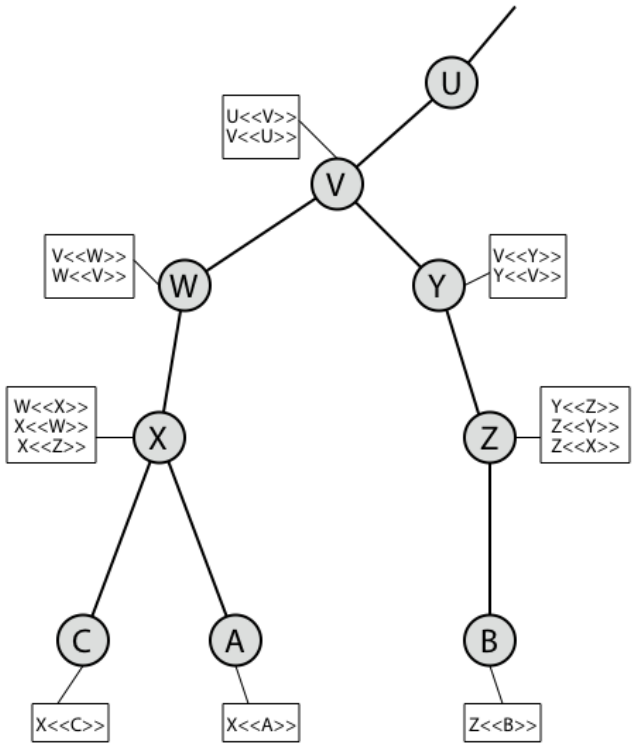
6.5.3. Sơ đồ phân cấp CA

Nếu cả hai người sử dụng chia sẻ chung CA thì họ được giả thiết là biết khoá công khai của CA đó. Ngược lại các CA cần tạo nên sơ đồ phân cấp để trao đổi chứng nhận với nhau. Sử dụng chứng nhận liên kết các thành viên của sơ đồ để có được chứng

nhận của các CA khác. Mỗi CA có thể gửi tiếp các chứng nhận của mình cho clients và có thể gửi lại chứng nhận của mình cho cha của nó. Mỗi client tin tưởng các chứng nhận của cha. Có thể kiểm chứng chứng nhận bất kỳ của một CA cho người sử dụng bằng các CA khác trong sơ đồ phân cấp.

Trong sơ đồ sau hai người sử dụng A và B không có CA chung, mỗi người yêu cầu chứng nhận của người khác sẽ được thư mục thiết lập dãy chứng nhận tương ứng.

- CA trực tiếp của A là X, do đó A yêu cầu chứng nhận B được cung cấp dãy chứng nhận: X<<W>> W<<V>> V<<Y>> Y<<Z>> Z<<B>>
- CA trực tiếp của B là Z, do đó B yêu cầu chứng nhận A được cung cấp dãy chứng nhận: Z<<Y>> Y<<V>> V<<W>> W<<X>> X<<A>>



6.5.4. Sự thu hồi chứng nhận

Giấy chứng nhận có chu kỳ sử dụng, có thể thu hồi trước thời hạn trong những trường hợp cần thiết như: khoá riêng của người sử dụng bị lộ, người dùng không tiếp tục được chứng nhận bởi CA đó, Giấy chứng nhận của CA bị làm hại. Nói chung CA bảo trì danh sách các chứng nhận bị thu hồi (CRL – Certificate Revocation List). Người sử dụng có thể kiểm tra lại các chứng nhận đã bị thu hồi.

6.5.5. Các thủ tục xác thực

X.509 bao gồm ba thủ tục xác thực tùy chọn: xác thực một chiều, xác thực hai chiều và xác thực ba chiều. Mọi thủ tục trên đều sử dụng các chữ ký khoá công khai.

Xác thực một chiều

Một chiều A->B được sử dụng để thiết lập:

- Danh tính của A và rằng mẩu tin là từ A.

- Mẩu tin được gửi cho B.
- Tính toàn vẹn và gốc gác của mẩu tin.

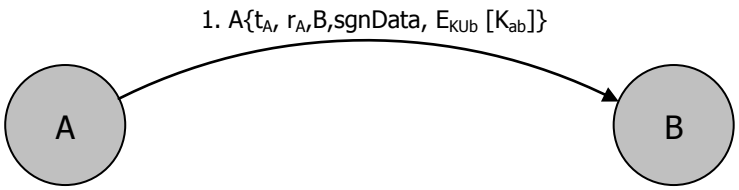
Mẩu tin có thể bao gồm cả nhãn thời gian, ký hiệu đặc trưng của mẩu tin (nonce), danh tính của B và nó được ký bởi A. Có thể bao gồm một số thông tin bổ sung cho B như khoá phiên.

Xác thực hai chiều

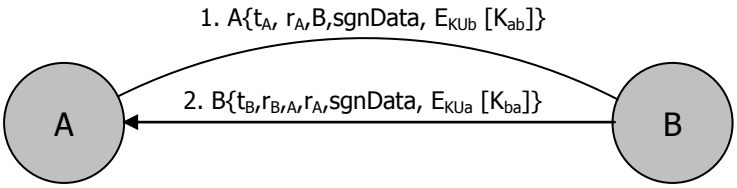
Hai mẩu tin A->B và B->A được thiết lập, ngoài mẩu tin từ A đến B như trên còn có:

- Danh tính của B và trả lời từ B.
- Trả lời này dành cho A.
- Tính toàn vẹn và gốc gác của trả lời.

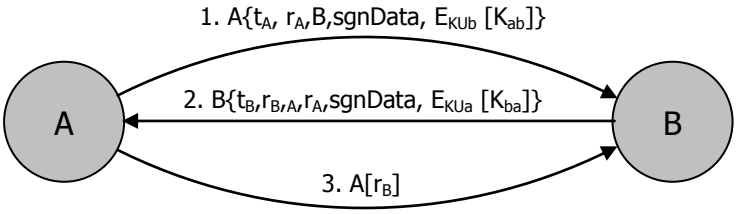
Trả lời bao gồm cả ký hiệu đặc trưng của mẩu tin (nonce) từ A, cả nhãn thời gian và ký hiệu đặc trưng trả lời từ B. Có thể bao gồm một số thông tin bổ sung cho A.



(a) One-way authentication



(b) Two-way authentication



(c) Three-way authentication

Xác thực ba chiều

Ba mẩu tin A->B, B->A và A->B được thiết lập như trên mà không có đồng hồ đồng bộ. Ngoài hai chiều như trên còn có trả lời lại từ A đến B chứa bản sao nonce của trả lời từ B. Thiết kế như vậy để các nhãn thời gian không cần kiểm tra, vì mỗi bên có thể kiểm tra các nonce phản hồi để chống tấn công lặp lại.

X.509 phiên bản 3

Trong phiên bản 3 được bổ sung một số thông tin cần thiết trong giấy chứng nhận như: Email/URL, chi tiết về đợt phát hành, các ràng buộc sử dụng. Tốt hơn hết là đặt tên tường minh cho các cột mới xác định trong phương pháp mở rộng tổng quát. Các mở rộng bao gồm:

- Danh tính mở rộng.
- Chỉ dẫn tính quan trọng.
- Giá trị mở rộng.
- Các mở rộng xác thực:
    - Khoá và các thông tin đợt phát hành;
    - Bao gồm thông tin về đối tượng, khoá người phát hành, chỉ thị kiểu phát hành, chứng nhận;
    - Đối tượng chứng nhận và các thuộc tính người phát hành;
    - Hỗ trợ có tên phụ, định dạng phụ cho các đối tượng và người phát hành;
    - Chứng nhận các ràng buộc phát hành;
    - Cho phép sử dụng các ràng buộc trong chứng nhận bởi các CA khác.

TÓM LƯỢC CUỐI BÀI

Chúng ta đã xem xét

- Phân phối và quản lý khóa công khai, khóa chính, khóa phiên.
- Hệ thống xác thực tin cậy Kerberos.
- Hạ tầng khóa công khai PKI.
- Hệ thống thư điện tử PGP.

CÂU HỎI TRẮC NGHIỆM CUỐI BÀI

1. Giải pháp nào là kém an toàn nhất để phân phối khóa công khai:
   A. Thông báo công khai
   B. Thư mục công cộng
   C. Chủ quyền khóa công khai
   D. Chủ quyền cấp giấy chứng nhận
2. Đâu là ưu điểm chính của Chủ quyền cấp giấy chứng nhận so với chủ quyền khóa công khai
   A. Chủ quyền khóa công khai cung cấp trực tuyến khóa công khai
   B. Chủ quyền chứng nhận cấp các giấy chứng nhận về khóa công khai
   C. Cả hai đều cho phép người sử dụng dễ dàng thay đổi khóa công khai của mình
   D. Chủ quyền khóa công khai dùng online, chủ quyền chứng nhận có thể offline

3. Giải pháp nào không dùng để phân phối công khai khóa mật giữa hai người sử dụng
   A. Dùng Trung tâm phân phối khóa KDC hỗ trợ phân phối khóa
   B. Trao đổi trực tiếp khóa mật dùng thủ tục trao đổi khóa Diffie-Helman
   C. Trao đổi khoá mật mới bằng khoá mật cũ
   D. Trao đổi trực tiếp khóa mật dùng khóa công khai
4. Trong phương pháp kết hợp phân phối khóa, điều nào không đúng
   A. Mỗi người sử dụng và Trung tâm phân phối khóa KDC có cặp khóa riêng và khóa công khai
   B. Trung tâm dùng khóa công khai để tạo khóa chính giữa KDC và mỗi NSD
   C. NSD dùng khóa công khai để trao đổi khóa phiên với NSD khác
   D. NSD dùng khóa chính để xin KDC tạo khóa phiên với NSD khác
5. Tự động phân phối khóa cho giao thức hướng đối tượng không sử dụng
   A. Máy chủ gửi gói tin kèm với yêu cầu kết nối với máy chủ khác
   B. Cả bên nhận và bên gửi cần thỏa thuận trước khoá phiên trước khi gửi gói tin
   C. Bộ xử lý đầu cuối lưu gói tin và yêu cầu KDC cấp khóa phiên
   D. KDC cấp khóa phiên cho cả hai bộ xử lý đầu cuối và sau đó mã hóa, rồi truyền gói tin lưu
6. Đối với Kerberos điều khẳng định nào sau đây không đúng:
   A. Hệ thống máy chủ xác thực tin cậy
   B. Xác thực một lần cho một phiên làm việc
   C. Cung cấp nhiều loại dịch vụ phân tán và kiểm soát quyền truy cập
   D. Mỗi lần sử dụng một dịch vụ trong hệ thống cần phải xác thực để kiểm soát quyền truy cập
7. Mục nào không phải là yêu cầu ban đầu của Kerberos:
   A. An toàn
   B. Tin cậy
   C. Xác thực tập trung
   D. Có thể mở rộng
8. Vấn đề nào không thuộc cải tiến của Kerberos 5
   A. Tạo khóa mã từ mật khẩu
   B. Gửi khóa phiên và thẻ được mã bởi khóa sinh từ mật khẩu
   C. Cấp thẻ và khóa truy cập vào các máy chủ ứng dụng
   D. Thêm yếu tố thời gian vào các khóa cho dịch vụ để chống dùng lặp lại
9. Mục nào không nằm trong qui trình xác thực của Kerberos
   A. Người dùng nhập vào tên truy cập và mật khẩu ở phía máy trạm
   B. Tên và mật khẩu sẽ được truyền đến máy chủ xác thực để kiểm tra
   C. Máy trạm gởi một thông điệp dưới dạng bản rõ đến AS để yêu cầu dịch vụ.
   D. AS kiểm tra xem có tồn tại người dùng trong cở sở dữ liệu của nó hay không. Nếu có, nó gởi ngược lại cho máy trạm thông điệp được mã bằng khóa sinh từ mật khẩu người dùng.
10. Điều nào không đúng với hạ tầng khóa công khai PKI
    A. Đây là thuật toán mã hóa công khai
    B. Đây là cơ chế quản lý và phân phối khóa công khai
    C. Giấy chứng nhận được ký bởi mã công khai của chủ quyền chứng nhận
    D. Có danh sách thu hồi các giấy chứng nhận
11. Đâu không phải là thành phần của hạ tầng khóa công khai
    A. Chủ quyền đăng ký CR
    B. Chủ quyền chứng nhận CA
    C. Chủ quyền khóa công khai
    D. Xuất bản danh sách thu hồi CRL
12. Đâu không phải là thao tác PGP

A. Bảo mật
B. Xác thực
C. Mã xác thực thông điệp
D. Nén và chuyển dữ liệu thành các ký tự in được

13. Sơ đồ tổng quát người gửi không bao gồm
A. Nếu có ký, thì ký rồi nén
B. Nén, rồi xét đến việc ký hay không
C. Sau nén, xét đến việc có bản mật hay không
D. Sau bảo mật sẽ dùng hàm chuyển R64
14. Trong chùm khóa riêng không có trường nào
A. Nhãn thời gian và khóa công khai
B. Mã khóa riêng
C. Khóa riêng
D. Mã người sử dụng
15. Trong chùm khóa công khai không có trường nào
A. Nhãn thời gian và khóa công khai
B. Mã khóa riêng
C. Mã người sử dụng
D. Chữ ký chứng nhận
16. Trong định dạng mẩu tin PGP không có trường nào.
A. Thành phần khóa phiên gồm mã khóa của khóa công khai người nhận
B. Thành phần chữ ký gồm nhãn thời gian, khóa công khai người gửi, ký bản băm
C. Thành phần mẩu tin
D. Thành phần số ngẫu nhiên
17. Trong quá trình sinh mẫu tin để gửi điều gì sau đây không đúng
A. Người gửi nhập mật khẩu, băm thành khóa giải mã khóa riêng
B. Người gửi ký bằng cách mã bản băm bằng khóa riêng
C. Người gửi dùng khóa phiên đã thỏa thuận để mã mẩu tin
D. Người gửi mã bằng khóa phiên sinh ngẫu nhiên và mã khóa phiên bằng khóa công khai của người nhận
18. Trong quá trình nhận mẫu tin điều gì sau đây không đúng
A. Người nhận nhập mật khẩu, băm thành khóa giải mã khóa riêng
B. Người nhận dùng khóa phiên đã thỏa thuận
C. Người nhận dùng khóa riêng giải mã lấy khóa phiên
D. Người nhận dùng khóa phiên giải mã mẩu tin hoặc dùng khóa công khai và băm bản tin để kiểm tra chữ ký

ĐÁP ÁN CÂU HỎI TRẮC NGHIỆM CUỐI BÀI

Câu 1: A, Thông báo công khai, cần phải chống mạo danh
Câu 2: D, Chủ quyền khóa công khai dùng online, chủ quyền chứng nhận có thể offline, nên không phụ thuộc
Câu 3: C, Không thể trao đổi khoá mật mới bằng khoá mật cũ, vì nếu khóa mật cũ đã lộ, thì không an toàn
Câu 4: Trong phương pháp kết hợp, có bên thứ 3 C, NSD dùng khóa chính chứ không phải khóa công khai để trao đổi khóa phiên với NSD khác thông qua KDC
Câu 5: B, Hai bên không cần thỏa thuận khóa phiên trước khi trao đổi
Câu 6: D, Mỗi lần sử dụng dịch vụ, không cần xác thực lại, vì đã được xác thực và cấp thẻ
Câu 7: C, Xác thực tập trung không phải yêu cầu ban đầu
Câu 8: C, Sử dụng thẻ và khóa đã có trong phiên bản trước

Câu 9: B, Mật khẩu không được truyền đến máy chủ để kiểm tra
Câu 10: A, Đây không phải là thuật toán, mà là hạ tầng gồm nhiều chức năng
Câu 11: C, Không có chủ quyền khóa công khai mà có chủ quyền chứng nhận CA
Câu 12: C, Không dùng mã xác thực mà dùng bản băm và ký bằng khóa riêng
Câu 13: B, Ký nếu có thì xảy ra trước nén
Câu 14: C, Không chứa khóa riêng dạng tường minh
Câu 15: C, Không chứa mã khóa riêng
Câu 16: C, Không chứa số ngẫu nhiên
Câu 17: C, Dùng khóa phiên sinh ngẫu nhiên rồi mã bằng khóa công khai người nhận
Câu 18: B, Không dùng khóa phiên thỏa thuận

THUẬT NGỮ TRONG BÀI

- Phân phối khóa công khai: cung cấp khóa công khai của người sử dụng một cách an toàn
- Thư mục công cộng: Thư mục có người quản trị để mọi người sử dụng đăng ký và chia sẻ khóa công khai
- Chủ quyền khóa công khai: Người có thẩm quyền quản trị và cung cấp khóa công khai trực tuyến, dùng mã khóa riêng ký nhận khóa công khai của người sử dụng
- Chủ quyền Giấy chứng nhận: Người có thẩm quyền quản trị khóa công khai và cung cấp Giấy chứng nhận khóa công khai của người sử dụng được ký bằng mã khóa riêng
- Khóa phiên (section key): Khóa tạm thời, dùng để mã hoá dữ liệu giữa nhóm người sử dụng cho một phiên logic và sau đó bỏ đi.
- Khóa chính (master key): khóa dùng để mã các khóa phiên, chia sẻ giữa người sử dụng và trung tâm phân phối khóa.
- Kerberos: Hệ thống máy chủ xác thực và cung cấp các dịch vụ phân tán được phát triển ở MIT.
- Hạ tầng khóa công khai PKI: Hệ thống cung cấp và quản lý Giấy chứng nhận về khóa công khai của người sử dụng
- An toàn thư điện tử nhằm đảm bảo các yêu cầu sau: tính bảo mật nội dung tin gửi, xác thực người gửi mẩu tin, tính toàn vẹn của mẩu tin, hơn nữa bảo vệ khỏi bị sửa, tính chống từ chối gốc, chống từ chối của người nhận.

CÂU HỎI THƯỜNG DÙNG

Câu 1. Ưu nhược điểm của việc quản lý khóa công khai bằng thư mục công cộng?
Câu 2. Ưu nhược điểm của việc quản lý khóa công khai bằng chủ quyền khóa công khai?
Câu 3. Ưu nhược điểm của việc quản lý khóa công khai bằng chủ quyền chứng nhận khóa công khai?
Câu 4. Giải thích sơ đồ trao đổi trực tiếp khóa mật dùng chung bằng khóa công khai?
Câu 5. Giải thích sơ đồ trao đổi khóa mật dùng chung bằng phương pháp kết hợp dùng khóa công khai với sự hỗ trợ của bên thứ ba?
Câu 6. Mục đích dùng khóa chính và khóa phiên là gì? Thời gian sử dụng chúng khác nhau như thế nào?
Câu 7. Nêu các vấn đề gặp phải khi giải quyết bài toán phân phối khóa?
Câu 8. Nêu mục đích và yêu cầu của hệ thống Kerberos?
Câu 9. Nêu cấu tạo mô hình Kerberos? Và việc yêu cầu dịch vụ trong lãnh địa khác được thực hiện như thế nào?
Câu 10. Mô tả giao thực xác thực sử dụng dịch vụ trong hệ thống Kerberos?
Câu 11. Kerberos phiên bản 5 có những cải tiến gì? Giải thích quá trình sinh khóa từ mật khẩu?
Câu 12. Mô tả hoạt động của cơ sở hạ tầng khóa công khai PKI?
Câu 13. Nêu các nhiệm vụ an ninh chính của Hệ thống thư điện tử?

Câu 14. Giải thích sơ đồ bảo mật và xác thực thư điện tử?
Câu 15. Mô tả các bước gửi một bức thư điện tử?
Câu 16. Mô tả các bước nhận một bức thư điện tử?

TRẢ LỜI CÂU HỎI THƯỜNG DÙNG

1. Thư mục có người quản trị kiểm soát quyền đăng ký và thay đổi, tuy vẫn còn lỗ hổng để giả mạo và sử đổi và phải hỗ trợ trực tuyến.
2. Chủ quyền Khóa công khai cung cấp khóa công khai có chử ký của Chủ quyền chống giả mạo và sửa đổi, nhưng vẫn hỗ trợ trực tuyến
3. Chủ quyền chứng nhận cấp Giấy chứng nhận có chữ ký chủ quyền, không cần trực tuyến
4. Trao đổi trực tiếp dùng khóa công khai: Lỗ hổng là thông điệp 4 dễ bị sử dụng lại của các lần trước đó, do không có nhãn thời gian
5. Trao đổi kết hợp với KDC: Thông điệp 3 vẫn có lỗ hổng, có thể bị dùng lặp, cần thêm nhãn thời gian, kéo theo vấn đề đồng hồ đồng bộ
6. Khóa chính trao đổi với KDC, ít thay đổi, Khóa phiên dùng cho phiên làm việc thay đổi thường xuyên, không có cơ hội phân tích cho kẻ thám mã.
7. Đối với mạng lớn đòi hỏi phân cấp Trung tâm phân phối khóa KDC, nhưng cần phải tạo tin cậy cho nhau, giữa người sử dụng với Trung tâm và các Trung tâm với nhau. Thời gian sống của khóa bộ phận cần được hạn chế để cho an toàn hơn. Sử dụng phân phối khóa tự động thay mặt người dùng, nhưng phải có hệ thống tin cậy, các khóa cấp phát được sinh ra càng ngẫu nhiên càng tốt.
8. Xác thực trung tâm, login một lần, an toàn, tin vậy, trong suốt, có thể mở rộng
9. Có máy chủ xác thực cấp thẻ cho phiên làm việc, máy chủ cấp thẻ cho các dịch vụ, có thể có nhiều lãnh địa
10. Xem bài giảng. Vấn đề là mật khẩu không truyền trên mạng và các thẻ phải được mã hóa, có yếu tố thời gian tránh dùng lại
11. Keberos 5 đã khắc phục các yếu điểm của Keberos 4 như dùng khóa sinh từ mật khẩu, mã kép, thêm nhãn thời gian
12. Nhiệm vụ của PKI:

- Quản lý danh tính người sử dụng (NSD) với khóa công khai
- Cấp chứng nhận của Chủ quyền Giấy chứng nhận CA cho NSD
- Huỷ và Thu hồi các giấy chứng nhận không còn hiệu lực
- Tạo ra Thư mục để lưu trữ các chứng nhận và danh sách thu hồi
- Cung cấp dịch vụ sẵn sàng cung cấp cho NSD như: đăng ký, truy cập, xin giấy chứng nhận, đưa ra danh sách thu hồi CRL

13. An toàn thư điện tử. Đảm bảo các yêu cầu sau: tính bảo mật nội dung tin gửi, xác thực người gửi mẩu tin, tính toàn vẹn của mẩu tin, hơn nữa bảo vệ khỏi bị sửa, tính chống từ chối gốc, chống từ chối của người nhận.

CÂU HỎI TỰ LUẬN

Câu 1. Ưu nhược điểm của việc quản lý khóa công khai bằng thư mục công cộng?

Câu 2. Ưu nhược điểm của việc quản lý khóa công khai bằng chủ quyền khóa công khai?

Câu 3. Ưu nhược điểm của việc quản lý khóa công khai bằng chủ quyền chứng nhận khóa công khai?

Câu 4. Giải thích sơ đồ trao đổi trực tiếp khóa mật dùng chung bằng khóa công khai?

Câu 5. Giải thích sơ đồ trao đổi khóa mật dùng chung bằng phương pháp kết hợp dùng khóa công khai với sự hỗ trợ của bên thứ ba?

Câu 6. Mục đích dùng khóa chính và khóa phiên là gì? Thời gian sử dụng chúng khác nhau như thế nào?

Câu 7. Nêu các vấn đề gặp phải khi giải quyết bài toán phân phối khóa?

Câu 8. Nêu mục đích và yêu cầu của hệ thống Kerberos?

Câu 9. Nêu cấu tạo mô hình Kerberos và việc yêu cầu dịch vụ trong lãnh địa khác được thực hiện như thế nào?

Câu 10. Mô tả giao thực xác thực sử dụng dịch vụ trong hệ thống Kerberos?

Câu 11. Kerberos phiên bản 5 có những cải tiến gì? Giải thích quá trình sinh khóa từ mật khẩu?

Câu 12. Mô tả hoạt động của cơ sở hạ tầng khóa công khai PKI?

Câu 13. Nêu các nhiệm vụ an ninh chính của Hệ thống thư điện tử?

Câu 14. Giải thích sơ đồ bảo mật thư điện tử?

Câu 15. Giải thích sơ đồ xác thực thư điện tử?

Câu 16. Mô tả các bước gửi một bức thư điện tử?

Câu 17. Mô tả các bước nhận một bức thư điện tử?

Câu 14. Nêu định dạng giấy chứng nhận X500?

Câu 15. Giải thích sơ đồ phân cấp chủ quyền chứng nhận CA?

Câu 16. Mô tả các thủ tục xác thực một chiều, hai chiều và ba chiều?

BÀI TẬP TRẮC NGHIỆM

1. **Giải pháp nào là kém an toàn nhất để phân phối khóa công khai?**
   A. Thông báo công khai;
   B. Thư mục công cộng;
   C. Chủ quyền khóa công khai;
   D. Chủ quyền cấp giấy chứng nhận.

2. **Đâu là ưu điểm chính của Chủ quyền cấp giấy chứng nhận so với chủ quyền khóa công khai?**
   A. Chủ quyền khóa công khai cung cấp trực tuyến khóa công khai;
   B. Chủ quyền chứng nhận cấp các giấy chứng nhận về khóa công khai;
   C. Cả hai đều cho phép người sử dụng dễ dàng thay đổi khóa công khai của mình;
   D. Chủ quyền khóa công khai dùng online, chủ quyền chứng nhận có thể offline.

3. **Giải pháp nào không dùng để phân phối công khai khóa mật giữa hai người sử dụng?**
   A. Dùng Trung tâm phân phối khóa KDC hỗ trợ phân phối khóa;
   B. Trao đổi trực tiếp khóa mật dùng thủ tục trao đổi khóa Diffie-Helman;
   C. Trao đổi khóa mật mới bằng khóa mật cũ;
   D. Trao đổi trực tiếp khóa mật dùng khóa công khai;

4. **Trong phương pháp kết hợp phân phối khóa, điều nào không đúng?**
   A. Mỗi người sử dụng và Trung tâm phân phối khóa KDC có cặp khóa riêng và khóa công khai;

B. Trung tâm dùng khóa công khai để tạo khóa chính giữa KDC và mỗi người sử dụng;
C. Người sử dụng dùng khóa công khai để trao đổi khóa phiên với người sử dụng khác;
D. Người sử dụng dùng khóa chính để xin KDC tạo khóa phiên với người sử dụng khác.

5. Tự động phân phối khóa cho giao thức hướng đối tượng không sử dụng

A. Máy chủ gửi gói tin kèm với cầu kết nối với máy chủ khác;
B. Cả bên nhận và bên gửi cần thỏa thuận trước khóa phiên trước khi gửi gói tin;
C. Bộ xử lý đầu cuối lưu gói tin và yêu cầu KDC cấp khóa phiên;
D. KDC cấp khóa phiên cho cả hai bộ xử lý đầu cuối và sau đó mã hóa, rồi truyền gói tin lưu.

6. Đối với Kerberos điều khẳng định nào sau đây không đúng?

A. Hệ thống máy chủ xác thực tin cậy;
B. Xác thực một lần cho một phiên làm việc;
C. Cung cấp nhiều loại dịch vụ phân tán và kiểm soát quyền truy cập;
D. Mỗi lần sử dụng một dịch vụ trong hệ thống cần phải xác thực để kiểm soát quyền truy cập.

7. Mục nào không phải là yêu cầu của Kerberos?

A. An toàn;
B. Tin cậy;
C. Xác thực tập trung;
D. Có thể mở rộng.

8. Vấn đề nào không thuộc cải tiến của Kerberos 5?

A. Tạo khóa mã từ mật khẩu;
B. Gửi khóa phiên và thẻ được mã bởi khóa sinh từ mật khẩu;
C. Cấp thẻ và khóa truy cập vào các máy chủ ứng dụng;
D. Thêm yếu tố thời gian vào các khóa cho dịch vụ để chống dùng lặp lại.

9. Mục nào không nằm trong quy trình xác thực của Kerberos?

A. Người dùng nhập vào tên truy cập và mật khẩu ở phía máy trạm;
B. Tên và mật khẩu sẽ được chuyển đến máy chủ xác thực để kiểm tra;
C. Máy trạm gửi một thông điệp dưới dạng bản rõ đến AS để yêu cầu dịch vụ;
D. AS kiểm tra xem có tồn tại người dùng trong cở sở dữ liệu của nó hay không. Nếu có, nó gửi ngược lại cho máy trạm thông điệp được mã bằng khóa sinh từ mật khẩu người dùng.

10. Mục nào không nằm trong qui trình sinh khóa từ mật khẩu?

A. Chuyển mật khẩu thành dòng bit;
B. Chuyển dòng bit thành khóa đầu vào;
C. Khoá đầu vào mã các khối mật khẩu theo chế độ dây chuyền tạo đầu ra 64 bit cộng XOR với khóa đầu vào tạo ra 64 bit làm khóa;
D. Khóa đầu vào mã các khối mật khẩu theo chế độ dây chuyền tạo đầu ra 64 bit làm khóa.

11. Điều nào không đúng với hạ tầng khóa công khai?

A. Đây là thuật toán mã hóa công khai;
B. Đây là cơ chế quản lý và phân phối khóa công khai;
C. Giấy chứng nhận được ký bởi mã công khai của chủ quyền chứng nhận;
D. Có danh sách thu hồi các giấy chứng nhận.

12. Đâu không phải là thành phần của hạ tầng khóa công khai?
A. Chủ quyền đăng ký CR;
B. Chủ quyền chứng nhận CA;
C. Chủ quyền khóa công khai;
D. Xuất bản danh sách thu hồi CRL.

13. Đâu không phải là thao tác PGP?
A. Bảo mật ;
B. Xác thực ;
C. Không đồng thời xác thực và bảo mật được;
D. Nén và chuyển dữ liệu thành các ký tự in được.

14. Sơ đồ tổng quát người gửi không bao gồm
A. Nếu có ký, thì ký rồi nén;
B. Nén, rồi xét đến việc ký hay không;
C. Sau nén, xét đến việc có bảo mật hay không;
D. Sau bảo mật sẽ dùng hàm chuyển R64.

15. Trong chùm khóa riêng không có trường nào?
A. Nhãn thời gian và khóa công khai;
B. Mã khóa riêng;
C. Khóa riêng;
D. Mã người sử dụng.

16. Trong chùm khóa công khai không có trường nào?
A. Nhãn thời gian và khóa công khai;
B. Mã khóa riêng;
C. Mã người sử dụng;
D. Chữ ký chứng nhận.

17. Trong định dạng mẩu tin PGP không có trường nào?
A. Thành phần khóa phiên gồm mã khóa của khóa công khai người nhận;
B. Thành phần chữ ký gồm nhãn thời gian, khóa công khai người gửi, ký bản băm;
C. Thành phần mẩu tin;
D. Thành phần các tham số.

18. Trong quá trình sinh mẩu tin để gửi điều gì sau đây không đúng?
A. Người gửi nhập mật khẩu, băm thành khóa để giải mã khóa riêng;
B. Người gửi ký bằng cách mã bản băm bằng khóa riêng;
C. Người gửi dùng khóa phiên đã thỏa thuận để mã mẩu tin;

D. Người gửi mã bằng khóa phiên sinh ngẫu nhiên và mã khóa phiên bằng khóa công khai của người nhận.

19. Trong quá trình nhận mẩu tin điều gì sau đây không đúng?

A. Người nhận nhập mật khẩu, băm thành khóa giải mã khóa riêng;

B. Người nhận lấy khóa phiên đã thỏa thuận;

C. Người nhận dùng khóa riêng giải mã lấy khóa phiên;

D. Người nhận dùng khóa phiên giải mã mẩu tin hoặc dùng khóa công khai và băm bản tin để kiểm tra chữ ký.