Servicio de movilidad mundial para Universidades e Institutos de investigación de México

José Luis Quiroz Arroyo
jquiroz@inictel-uni.edu.pe
INICTEL-UNI

Javier Richard Quinto Ancieta
richardqa@gmail.com
INICTEL-UNI

México
10 – 13 de noviembre 2014

Lunes 10 de noviembre

UNIDAD I

Agenda: Lunes 10

Unidad I. Servidor RADIUS LOCAL

- **I.1 Introducción: Visión general de eduroam (45')**
- **I.2 Protocolo RADIUS: Aspectos generales (30')**
- **I.3 Practica 1:**
  - Configurar una Autoridad Certificadora privada y creación de certificados digitales usando OpenSSL (60').
  - Generar claves GPG para el intercambio de claves cifradas (45')
  - Creación de usuarios con autenticación simple usando los protocolos PAP y CHAP (15').
  - Configuración de los clientes RADIUS en el servidor local (institucional) (15').
- **I.4 Evaluación 1:**
  - Autenticación remota simple usando *radtest* entre servidores RADIUS (30') (20%)

I.1 Introducción

VISIÓN GENERAL DE EDUROAM

I.2 Aspectos generales

PROTOCOLO RADIUS

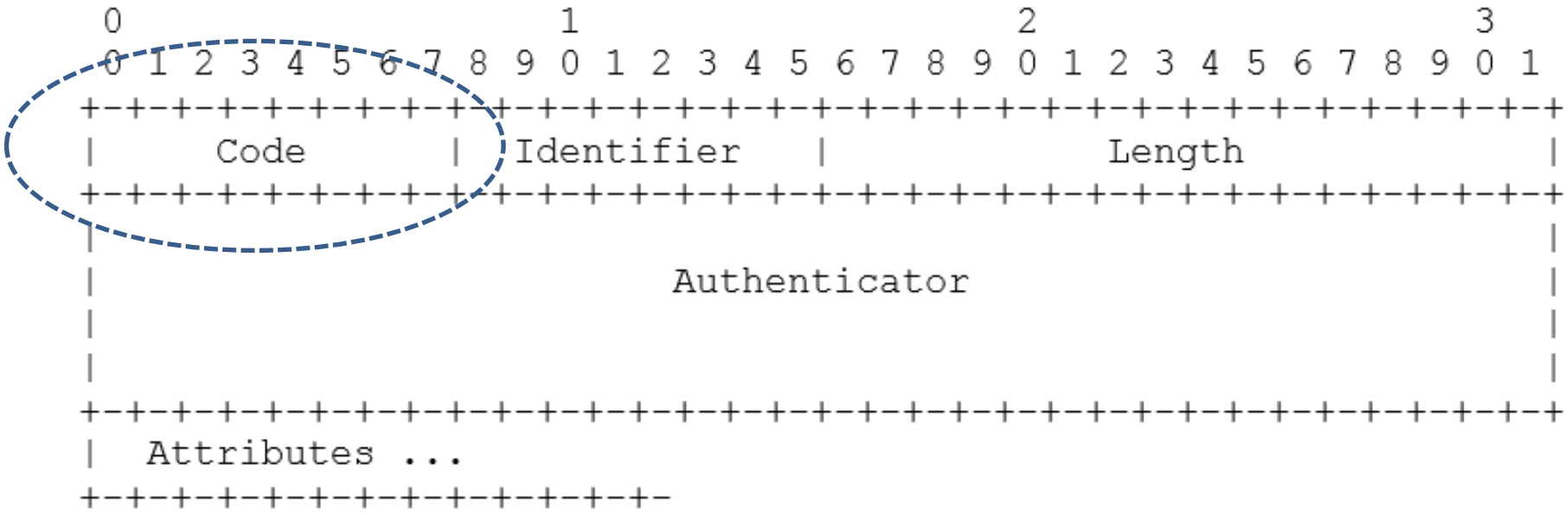
Protocolo RADIUS

- **RADIUS: Remote Authenticaion Dial In User Service (RFC 2865, 2866, 2867, 2868)**
  - Desarrollado por Livingston Enterprises
  - Es un protocolo AAA (Authentication, Authorization and Accounting), estándar abierto de IETF
  - Pensado para aplicaciones locales y de roaming
  - Es escalable: servidores Proxy
  - Soporta tecnología de acceso remoto: IEEE 802.1X

Qué hace?

- **Encripta solo el password**
  - RADIUS esconde los passwords durante la transmisión, incluso con el PAP (Password Authenticaion Protocol), mediante una operación compleja que involucra MD5 (Messge Digest) y un secreto compartido. El resto del paquete se envía en texto plano.
- **Los servicios de Autenticación y Autorización son combinados como un solo proceso**
  - Cuando un usuario está autenticado, el usuario también esta autorizado.
  - RADIUS usa el puerto UDP 1812 para la autenticación y el puerto UDP 1813 para la contabilidad.

Formato del mensaje RADIUS



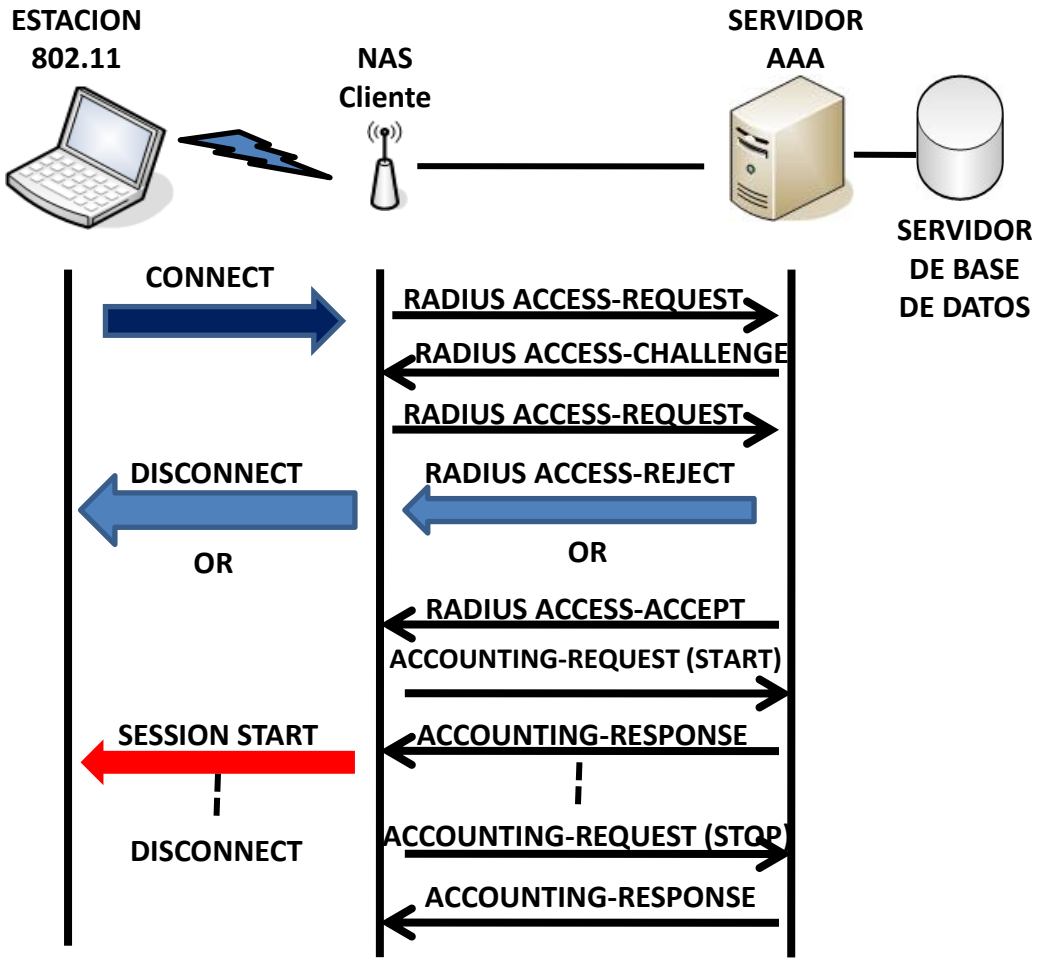
Campos de los mensajes RADIUS

- **Code (1 byte): Identifica el tipo de paquete RADIUS. Code (decimal):**
  - **1 Access-Request**: Paquetes enviados del NAS al servidor RADIUS, y transmiten información usada para determinar si se permite a un usuario el acceso a un NAS específico, y cualquier servicio especial solicitado por este usuario.
  - **2 Access-Accept**: Paquetes enviados por el servidor RADIUS al NAS, y proporcionan información de configuración específica necesaria para empezar la entrega de servicio al usuario (inicio de acceso).
  - **3 Access-Reject:** Paquetes enviados al NAS rechazando la autenticación o autorización. Indica que cualquier valor de los atributos recibidos no es aceptable.

Campos de los mensajes RADIUS

- **Code (1 byte): Identifica el tipo de paquete RADIUS. Code (decimal):**
  - 4 Accounting-Request: Se verá más adelante
  - 5 Accounting-Response: Se verá más adelante
  - **11 Access-Challenge:** Paquete enviado del servidor RADIUS al NAS. Si el servidor RADIUS desea enviar al usuario un reto requiriendo una respuesta, entonces el servidor RADIUS debe responder al Access-Request a través de la transmisión de un paquete con el campo Code establecido a 11.
  - 12 Status-Server:
  - 13 Status-Client:
  - 255 Reserved

Funcionamiento de eduroam: Proceso de Autenticación y Accouting RADIUS

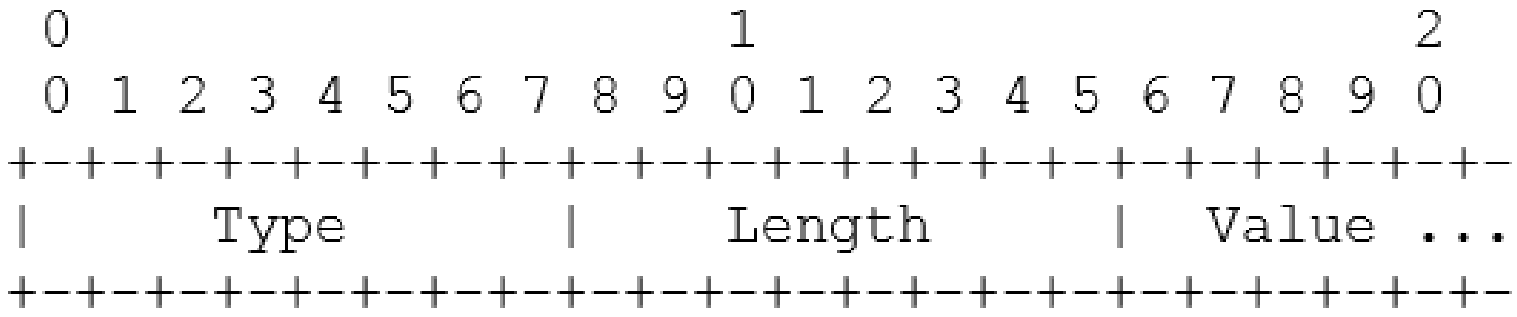


Campos de los mensajes RADIUS

- **Identifier (1 byte):**
  - Ayuda en coincidir los `request` y `replies`. El servidor RADIUS puede detectar una solicitud duplicada si tiene la misma dirección IP de origen de cliente, el puerto UDP de origen y el identificador dentro de un pequeño espacio de tiempo.
- **Length (2 bytes):**
  - Longitud del paquete incluyendo *Code, Identifier, Length, Authenticator y Attribute*
- **Authenticator (16 bytes):**
  - Un byte más significativo es transmitido primero. Este valor autentica la respuesta desde el servidor RADIUS, y es usado en el algoritmo de ocultación de password.

Campos de los mensajes RADIUS

- **Attributes**
  - Llevan la autenticación específica, autorización, información y los detalles de configuración para los **`request`** y **`reply`**



Campos de los mensajes RADIUS

- **Attributes:** La especificación de tipo se refiere a los siguientes valores:

1	User-Name	15	Login-Service	29	Termination-Action
2	User-Password	16	Login-TCP-Port	30	Called-Station-Id
3	CHAP-Password	17	(unassigned)	31	Calling-Station-Id
4	NAS-IP-Address	18	Reply-Message	32	NAS-Identifier
5	NAS-Port	19	Callback-Number	33	Proxy-State
6	Service-Type	20	Callback-Id	34	Login-LAT-Service
7	Framed-Protocol	21	(unassigned)	35	Login-LAT-Node
8	Framed-IP-Address	22	Framed-Route	36	Login-LAT-Group
9	Framed-IP-Netmask	23	Framed-IPX-Network	37	Framed-AppleTalk-Link
10	Framed-Routing	24	State	38	Framed-AppleTalk-Network
11	Filter-Id	25	Class	39	Framed-AppleTalk-Zone
12	Framed-MTU	26	Vendor-Specific	40-59	(reserved for accounting)
13	Framed-Compression	27	Session-Timeout	60	CHAP-Challenge
14	Login-IP-Host	28	Idle-Timeout	61	NAS-Port-Type
				62	Port-Limit
				63	Login-LAT-Port

Campos de los mensajes RADIUS

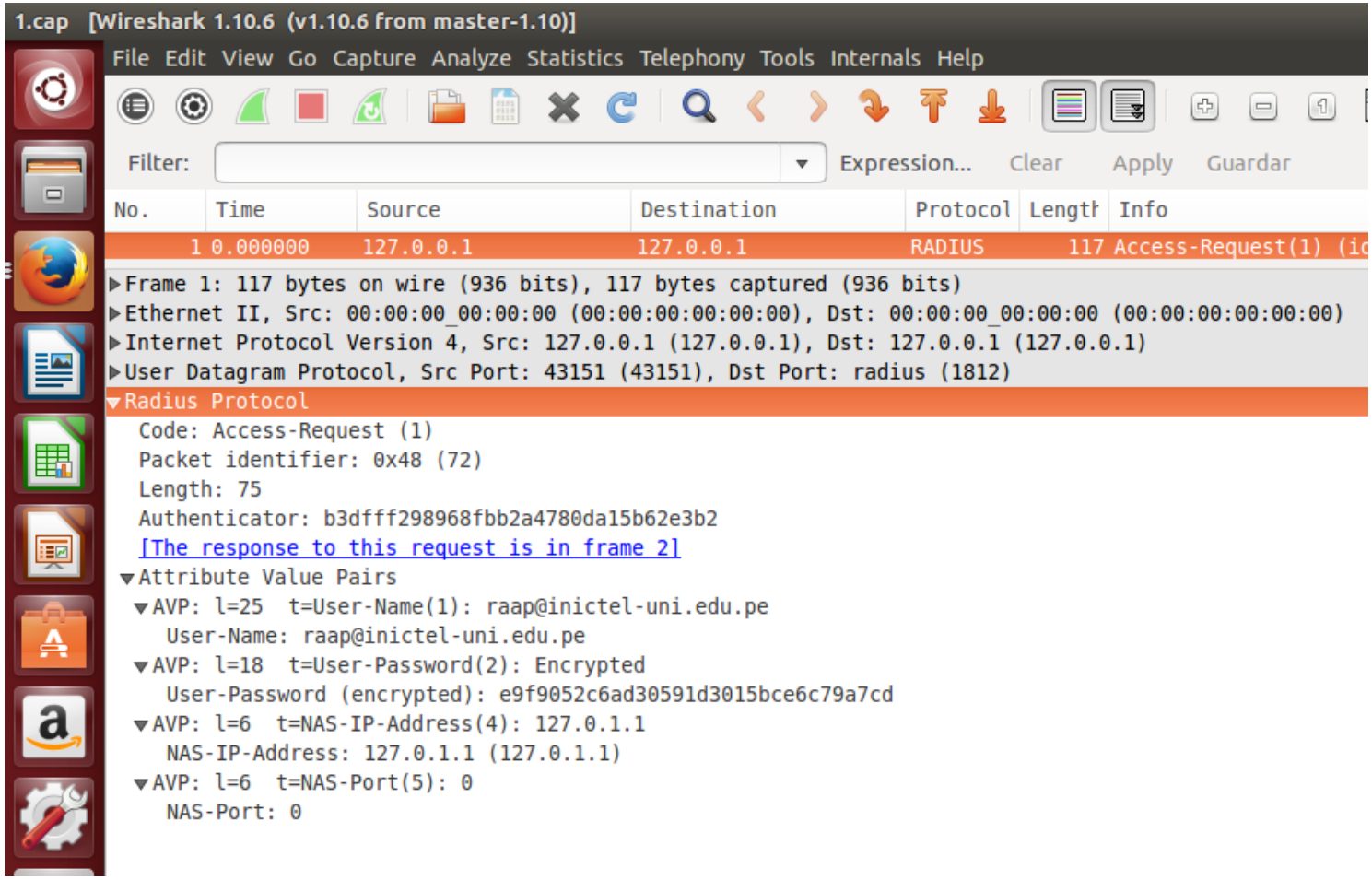
- **Attributes:**
  - Algunos Atributos a reconocer en eduroam

1	User-Name
2	User-Password
3	CHAP-Password
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
….	
14	Login-IP-Host
15	Login-Service
….	
32	NAS-Identifier
33	Proxy-State

Atributo User-Password

- **Indica el password del usuario a ser autenticada, o que la entrada del usuario sigue un `Access-Challenge`.**
  - Solamente es usada en los paquetes **`Access-Request`**.
  - En una transmisión, el password esta oculto.
  - La contraseña se rellena primero en el extremo con *ceros* a un múltiplo de 16 bytes. Se calcula un hash MD-5 de un solo sentido sobre un flujo (stream) de octetos que consiste del secreto compartido seguido por el **`Request Authenticator`**.
  - Este valor es XOR(reado) con el primer segmento de 16 bytes del password y colocado en los primeros 16 bytes del campo *String* (cadena) del atributo User-Password.

Ejemplo


1.cap [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter: Expression... Clear Apply Guardar
No. Time Source Destination Protocol Length Info
1 0.000000 127.0.0.1 127.0.0.1 RADIUS 117 Access-Request(1) (id
Frame 1: 117 bytes on wire (936 bits), 117 bytes captured (936 bits)
Ethernet II, Src: 00:00:00_00:00:00 (00:00:00:00:00:00), Dst: 00:00:00_00:00:00 (00:00:00:00:00:00)
Internet Protocol Version 4, Src: 127.0.0.1 (127.0.0.1), Dst: 127.0.0.1 (127.0.0.1)
User Datagram Protocol, Src Port: 43151 (43151), Dst Port: radius (1812)
Radius Protocol
Code: Access-Request (1)
Packet identifier: 0x48 (72)
Length: 75
Authenticator: b3dfff298968fbb2a4780da15b62e3b2
[The response to this request is in frame 2]
Attribute Value Pairs
AVP: l=25 t=User-Name(1): raap@inictel-uni.edu.pe
User-Name: raap@inictel-uni.edu.pe
AVP: l=18 t=User-Password(2): Encrypted
User-Password (encrypted): e9f9052c6ad30591d3015bce6c79a7cd
AVP: l=6 t=NAS-IP-Address(4): 127.0.1.1
NAS-IP-Address: 127.0.1.1 (127.0.1.1)
AVP: l=6 t=NAS-Port(5): 0
NAS-Port: 0

Comandos en FreeRADIUS

- **Comandos comúnes:**
  - freeradius (demonio)
  - freeradius –X (debug)
  - radtest (herramienta de autenticación: envía paquetes al servidor RADIUS, muestra la respuesta)
    - -t pap/chap/mschap/eap-md5
    - user
    - password
    - radius-server
  - eapol_test (prueba de autenticación)

ASPECTO TECNICO

Tareas

- Configurar el servidor RADIUS Local (RS-Local)
- Realizar pruebas de validación entre:

RS-LOCAL ← →FTLR-mx ←→RPS-LA←→ ETLR

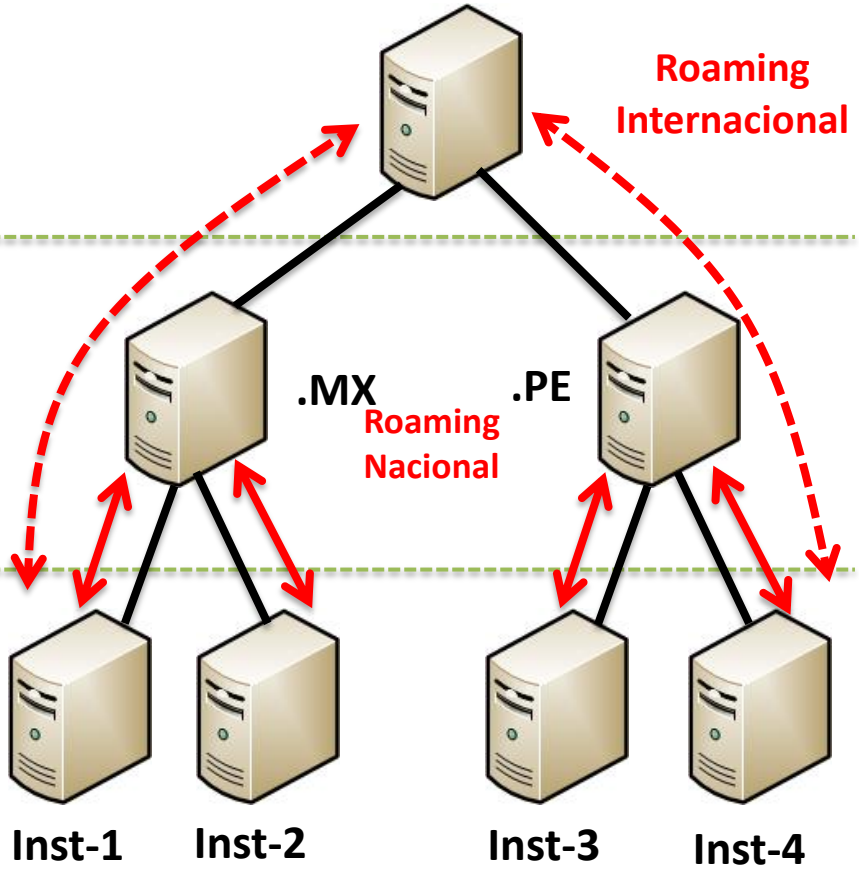
Infraestructura de eduroam

Jerarquía RADIUS

Nivel Confederación LTR

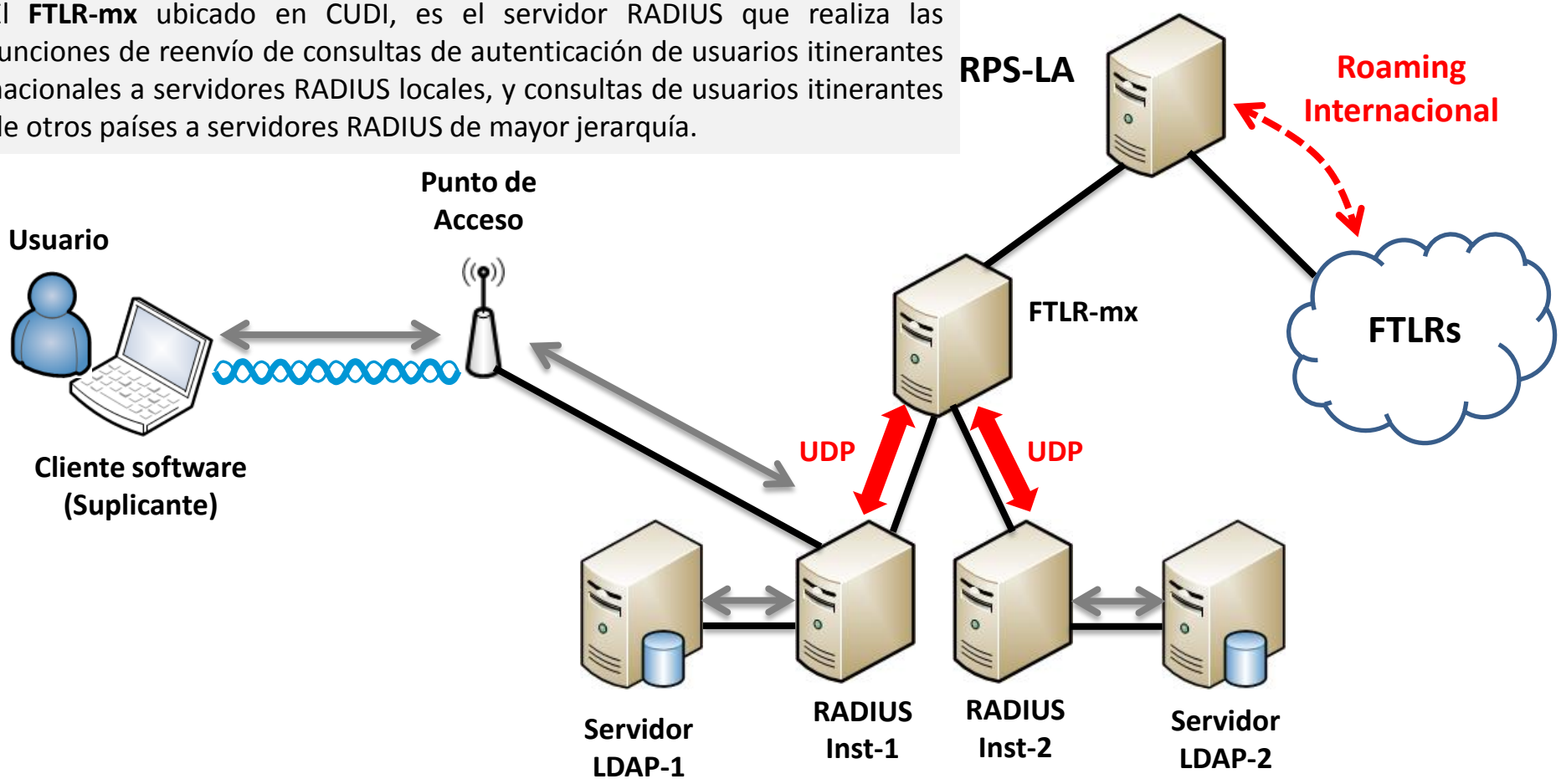
Nivel Federación FTLR

Nivel Institucional RS-LOCAL



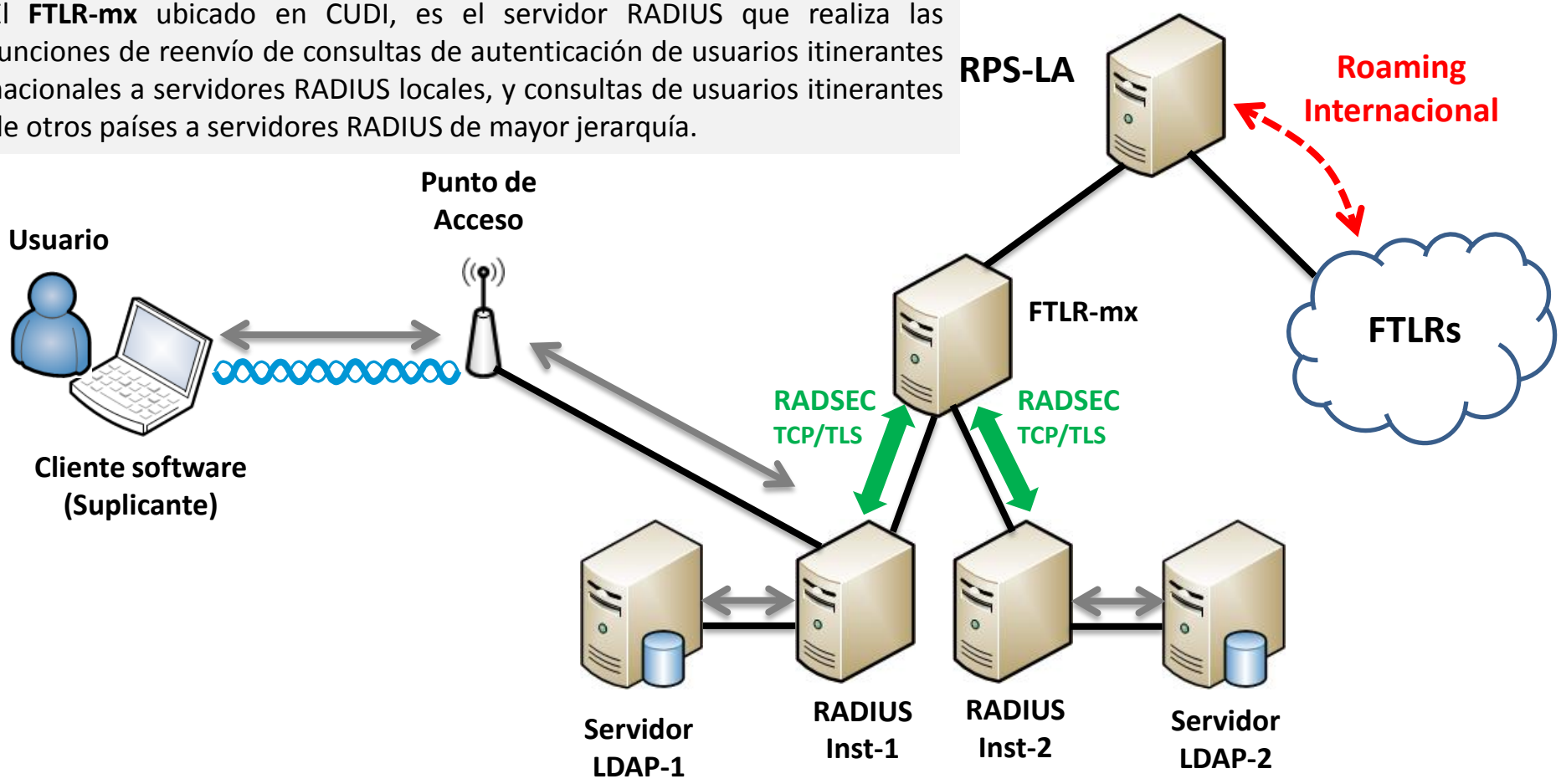
Infraestructura de eduroam: RADIUS

El **FTLR-mx** ubicado en CUDI, es el servidor RADIUS que realiza las funciones de reenvío de consultas de autenticación de usuarios itinerantes nacionales a servidores RADIUS locales, y consultas de usuarios itinerantes de otros países a servidores RADIUS de mayor jerarquía.



Infraestructura de eduroam: RADSEC

El **FTLR-mx** ubicado en CUDI, es el servidor RADIUS que realiza las funciones de reenvío de consultas de autenticación de usuarios itinerantes nacionales a servidores RADIUS locales, y consultas de usuarios itinerantes de otros países a servidores RADIUS de mayor jerarquía.



¿Cuál es el proceso de adherencia?

- **Paso 1.- Configurar un Servidor Radius Local de IdP**
  - Conseguir los “Accept” ejecutando *radtest*
- **Paso 2.- Registrarlo en la configuración del Servidor FTLR-mx**

(RS-LOCAL) --> FTLR-mx

- **Paso 3.- Realizar el protocolo de pruebas**

Protocolo de pruebas

- **Pruebas de autenticación RS-LOCAL < -- > FTLR-mx**
  - A nivel servidor y de usuarios ficticios.
  - El RS-LOCAL debe tener su enlace con una base de datos de usuarios (LDAP):
    - El éxito en este punto garantiza que los usuarios relacionados al RS-LOCAL puedan tener servicio de movilidad *eduroam*, previa configuración de clientes en dispositivos móviles.
- **Pruebas desde el FTLR-mx <--> RPS-LA <--> FTLR-tld**
  - A nivel servidor y de usuarios ficticios.

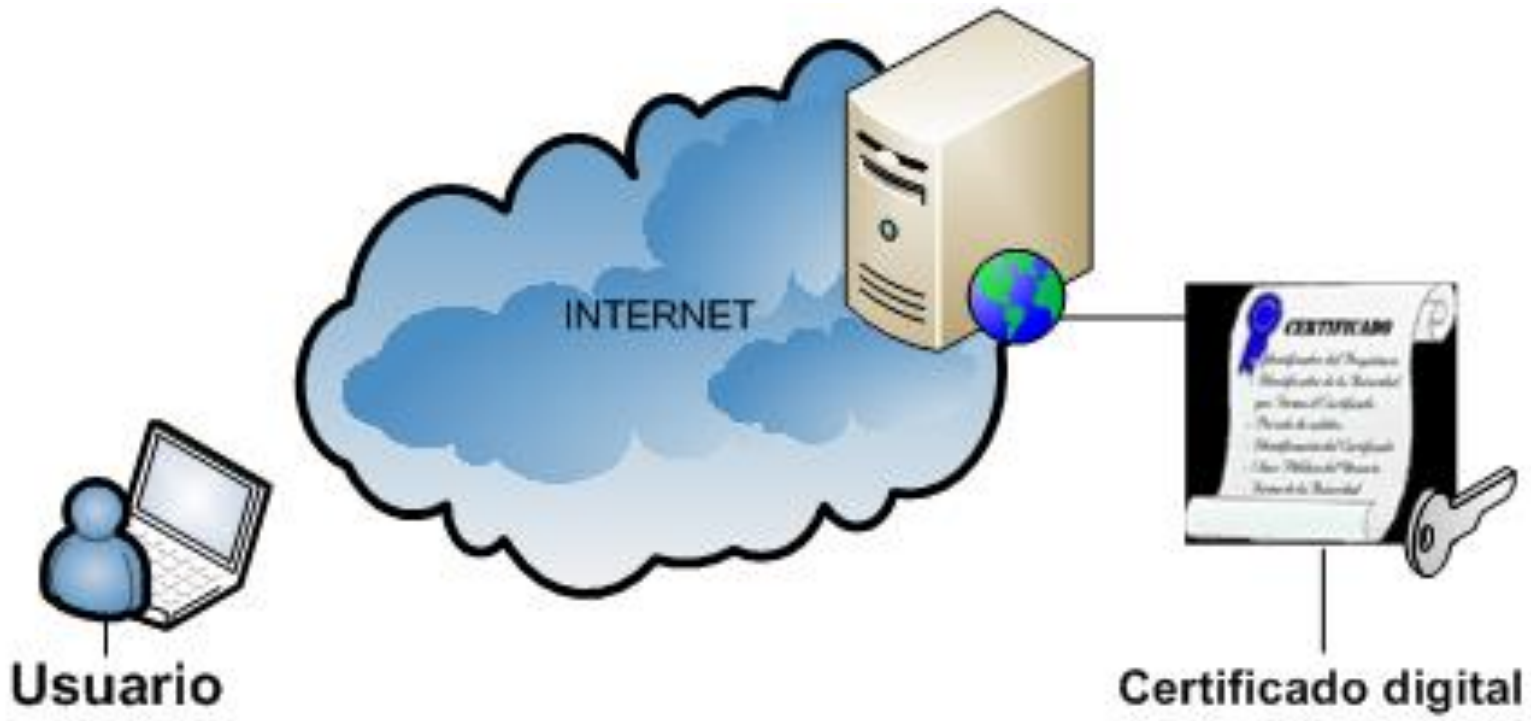
I.3 PRACTICA 1

Actividades: Lunes 10

Unidad I. Servidor RADIUS LOCAL

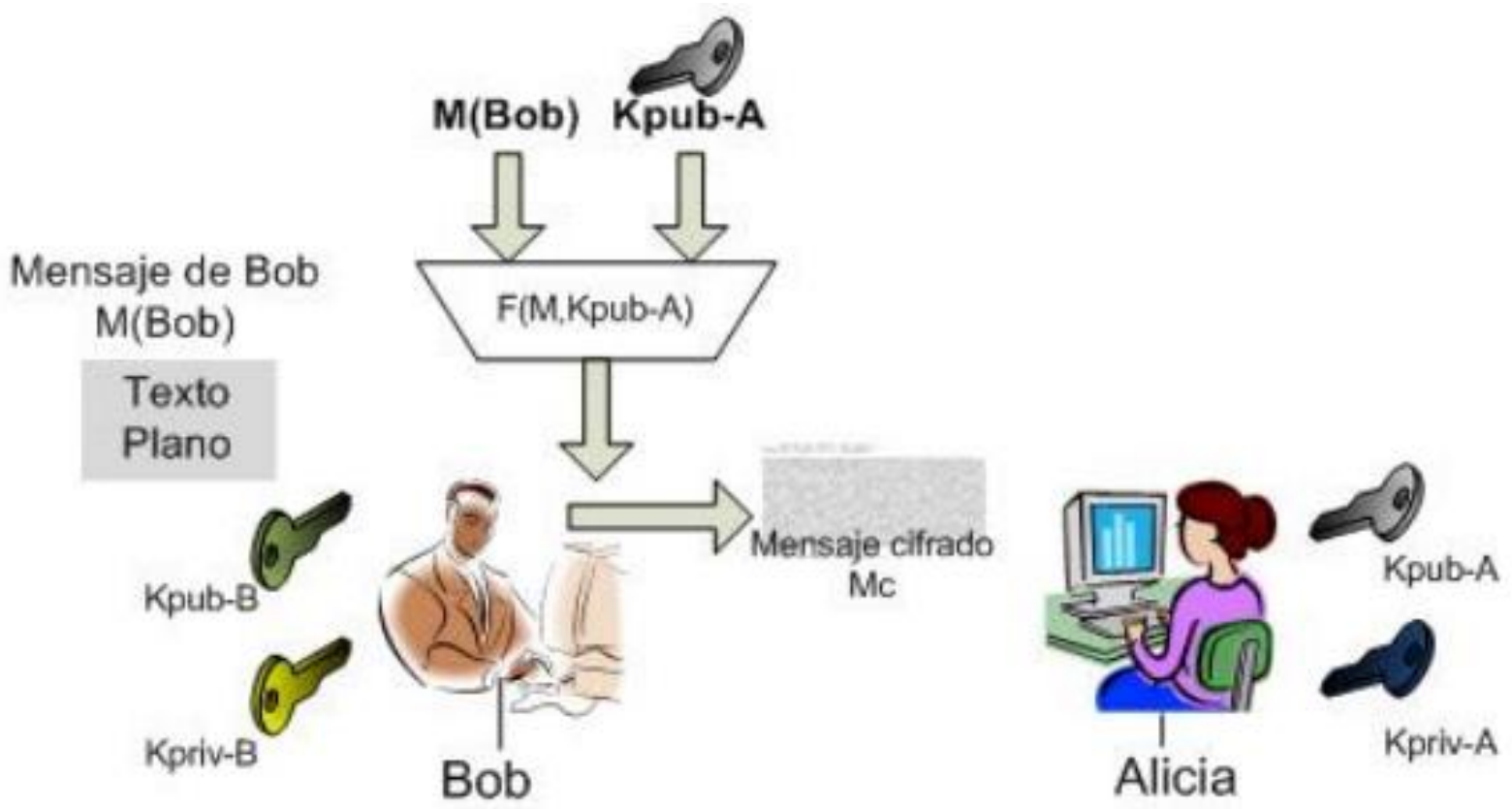
- **Los participantes configurarán remotamente su servidor RADIUS Local a través de una conexión SSH.**
  - Seguir las indicaciones del manual.
- **I.3 Practica 1:**
  - Configurar una Autoridad Certificadora privada y creación de certificados digitales usando OpenSSL (60').
  - Generar claves GPG para el intercambio de claves cifradas (45')
  - Creación de usuarios con autenticación simple usando los protocolos PAP y CHAP (15').
  - Configuración de los clientes RADIUS en el servidor local (institucional) (15').
- **I.4 Evaluación 1:**
  - Autenticación remota simple usando *radtest* entre servidores RADIUS (30') (20%)

Certificados Digitales



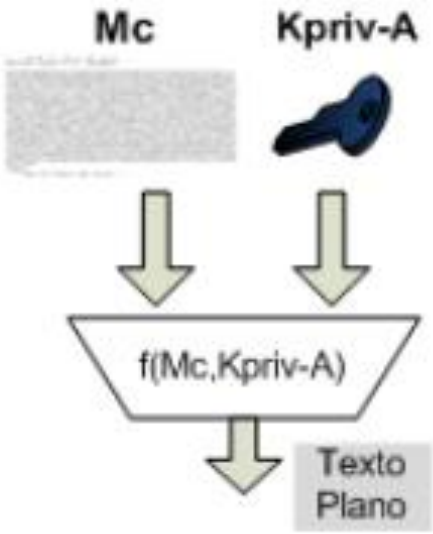
Criptografía Asimétrica (1/2)

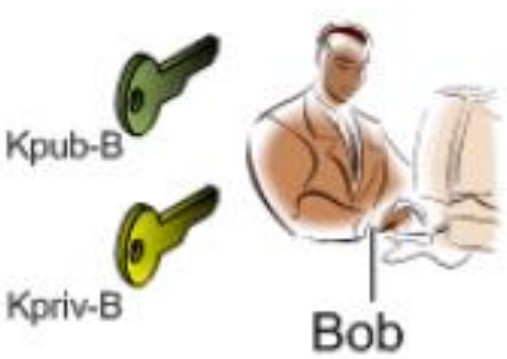
- **INTEGTRIDAD Y CONFIDENCIALIDAD**

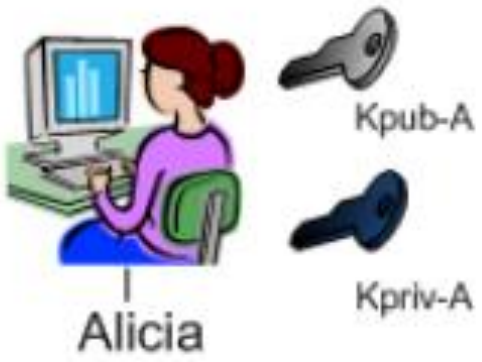


Criptografía Asimétrica (2/2)

- **INTEGTRIDAD Y CONFIDENCIALIDAD**

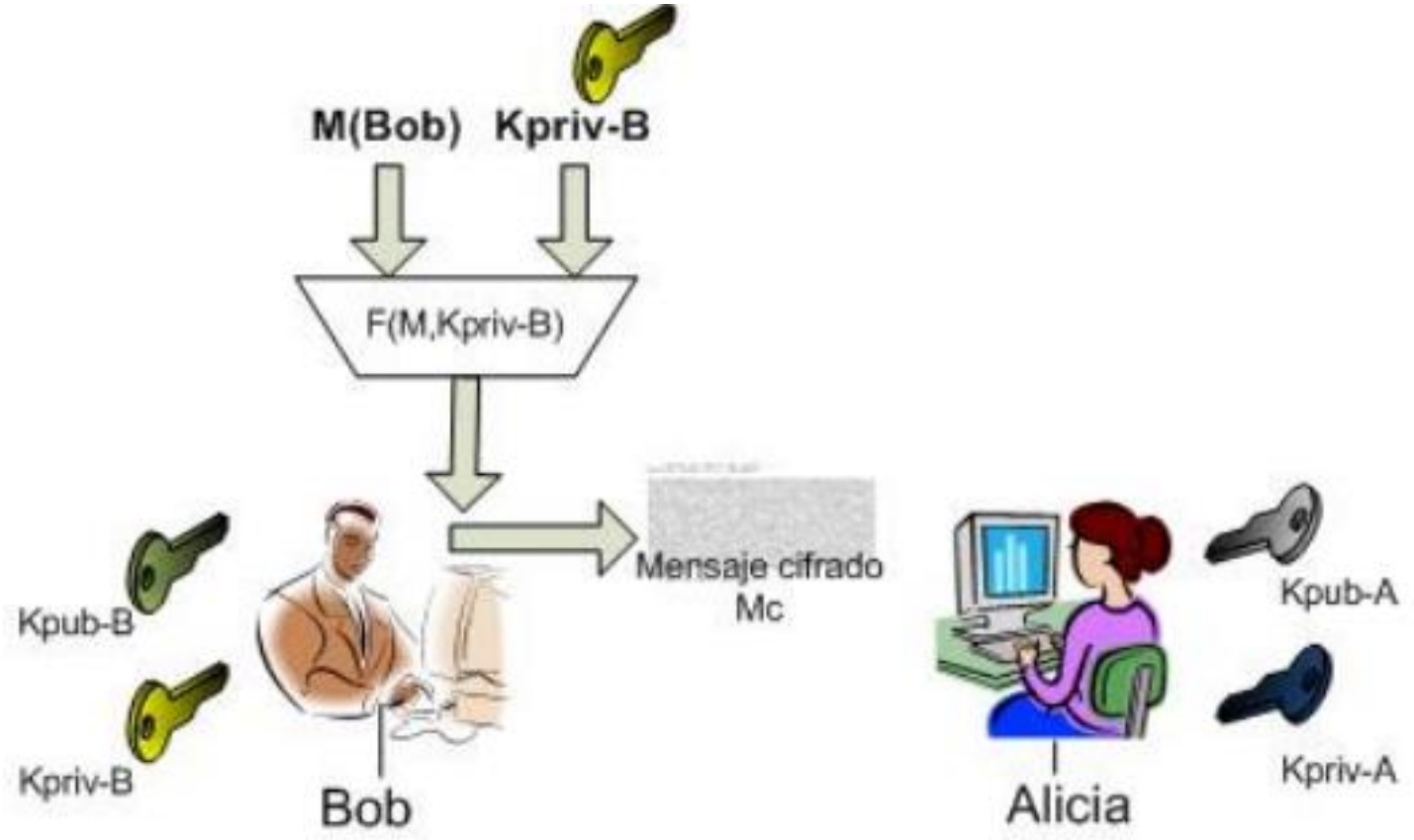






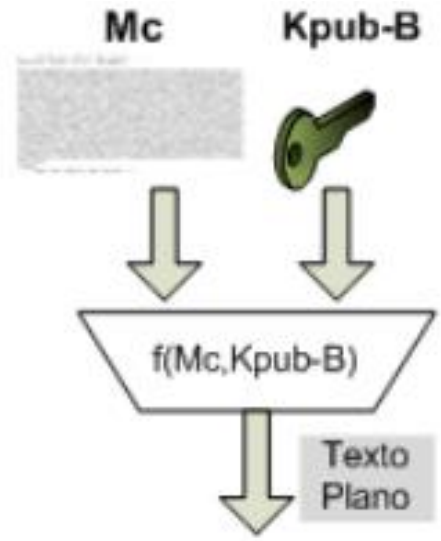
Criptografía Asimétrica (1/2)

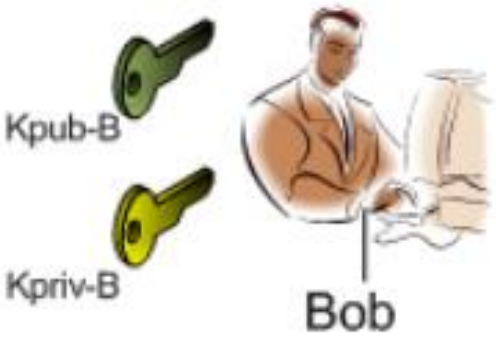
- **AUTENTICACION Y NO REPUDIO**



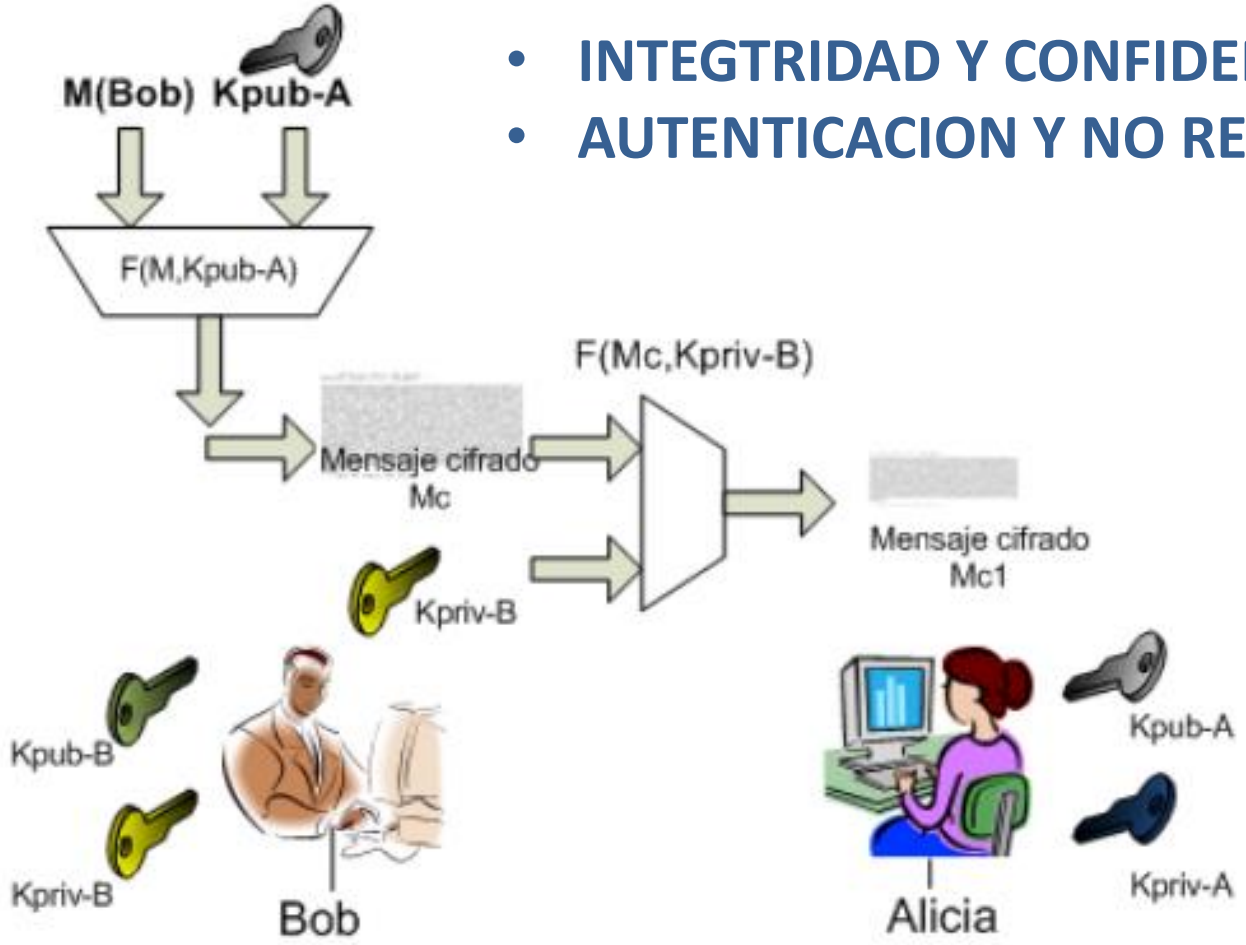
Criptografía Asimétrica (2/2)

- **AUTENTICACION Y NO REPUDIO**



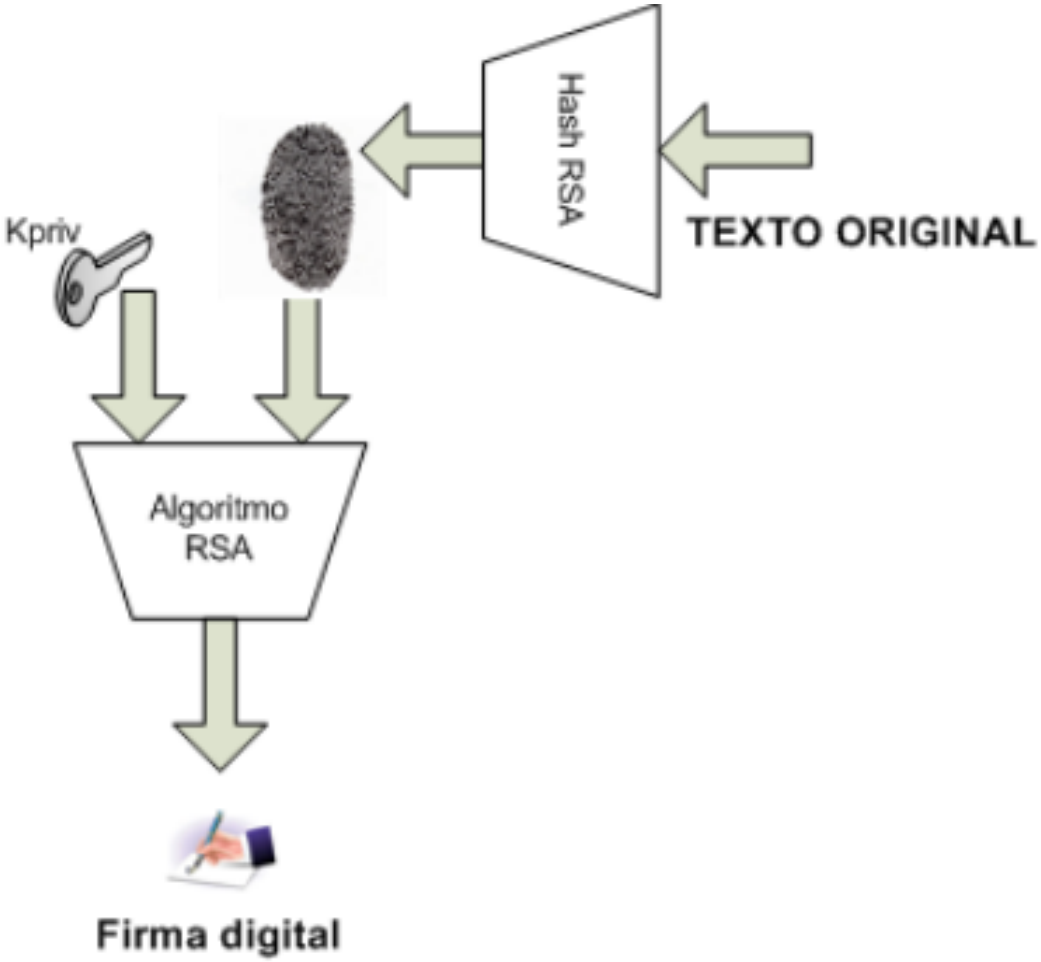


Criptografía Asimétrica

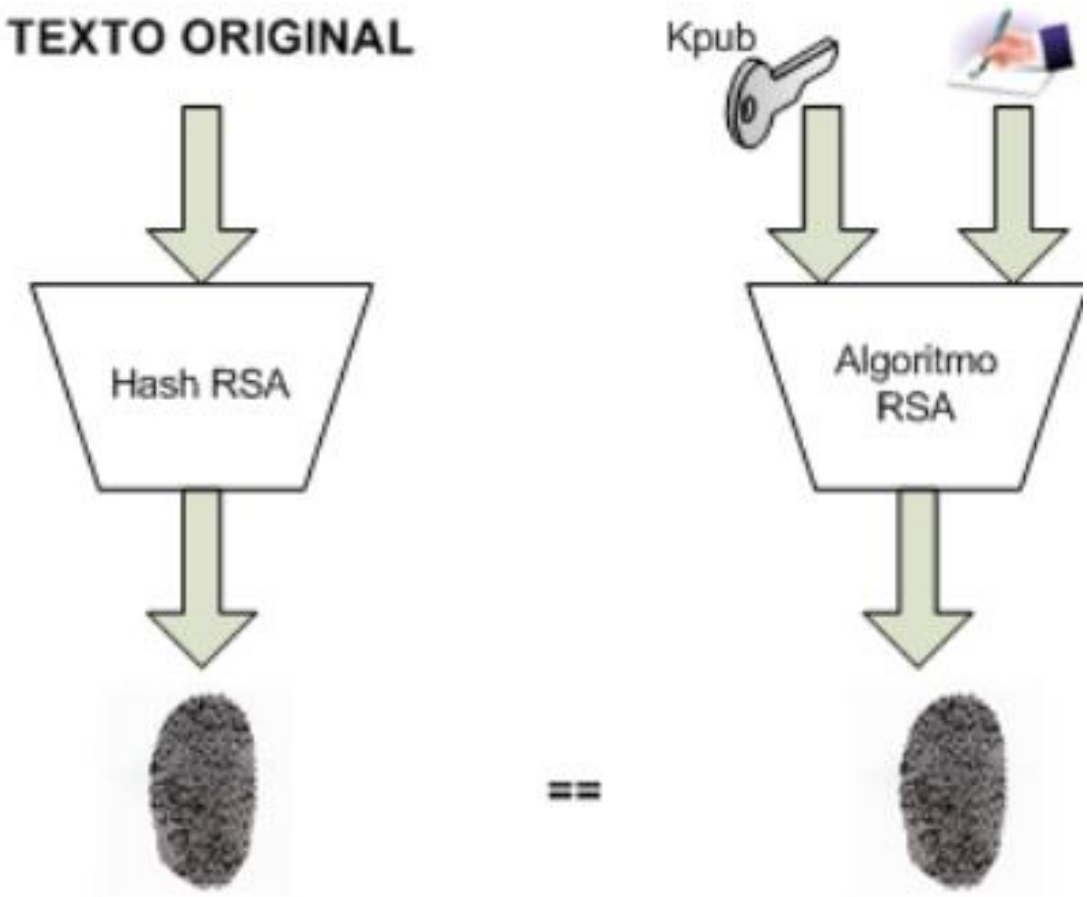


- **INTEGTRIDAD Y CONFIDENCIALIDAD**
- **AUTENTICACION Y NO REPUDIO**

Firma Digital

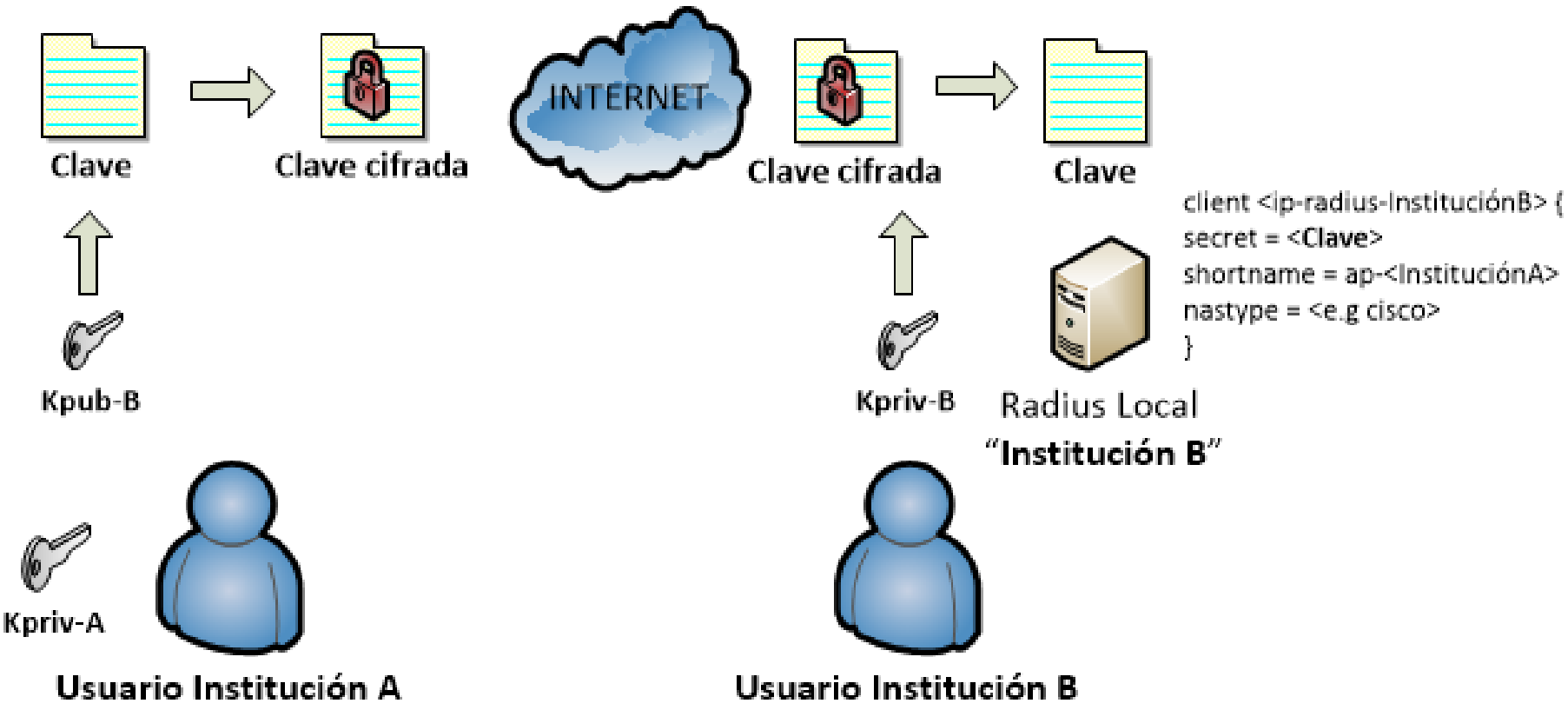


Comprobación de una Firma Digital



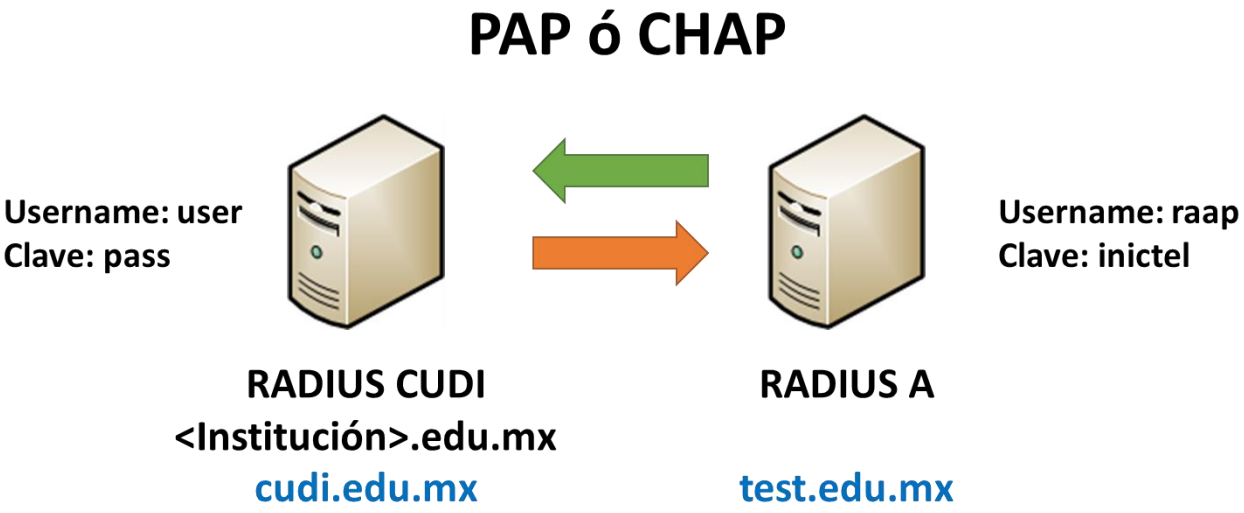
Infraestructura de Clave Pública

Intercambio de claves de forma segura usando GPG



Evaluación 1

Autenticación remota simple usando “radtest” entre servidores RADIUS (30’) (10%)



Enlaces de interés

- https://www.eduroam.org/
- http://www.eduroam.pe/
- http://www.inictel-uni.edu.pe/eduroam/main.html
- http://www.elcira.eu/

Muchas gracias!

jquiroz@inictel-uni.edu.pe

… desplegándose en Latino América