MOONSHOT

Acceso Federado Basado en GSS-API

Jornadas técnicas de RedIRIS 2012, Bilbao

Alejandro Pérez, Fernando Pereñíguez, Rafael Marín, Gabriel López

Departamento de Ingeniería de la Información y las Comunicaciones
Universidad de Murcia

Tabla de contenidos

1. Introducción
2. Moonshot
3. Moonshot & Kerberos
    1. Pre-autenticación Kerberos basada en GSS-EAP
    2. Pre-autenticación Kerberos basada en el acceso a la red
    3. Bootstrapping Kerberos basado en PANA

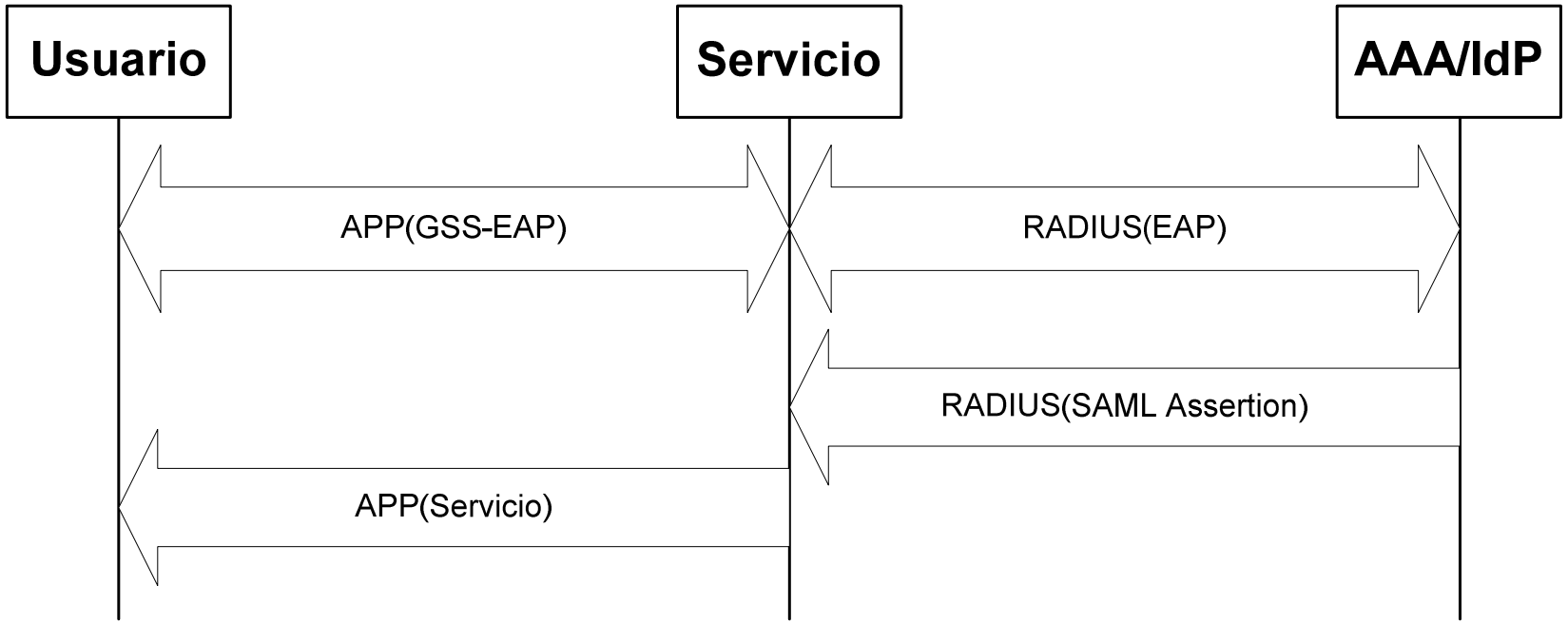
Introducción

- Federaciones de identidad
  - Relaciones de confianza para identificar usuarios
  - Usabilidad y menor coste de despliegue
- Inconvenientes
  - Definidas para tipos de servicio específicos
  - Uso de tecnologías diferentes
    - Acceso a la red (p.ej. eduroam) → RADIUS, Diameter...
    - Servicios web → SAML, OpenID…
  - Algunos servicios no disponen de soluciones de federación
    - Correo electrónico, acceso remoto a ficheros, acceso a terminal remoto…

Moonshot

- Realizado en parte dentro del proyecto GÉANT
  - Participado por RedIris
- Desarrollo de una tecnología para llevar el concepto de identidad federada a cualquier tipo de servicio
  - Uso de GSS-API como interfaz hacia los servicios
    - Ampliamente soportado (ej SSH, FTP, NTFS, HTTP…)
  - Uso de la infraestructura AAA como soporte de la federación
    - Uso de EAP como protocolo de autenticación
    - Definido un nuevo mecanismo GSS-API → GSS-EAP
  - Uso de SAML para autorización
    - Servicio obtiene una sentencia SAML con información sobre el usuario autenticado
    - Generado el IdP de la organización origen

Moonshot


Usuario
Servicio
AAA/IdP
APP(GSS-EAP)
RADIUS(EAP)
RADIUS(SAML Assertion)
APP(Servicio)

Moonshot

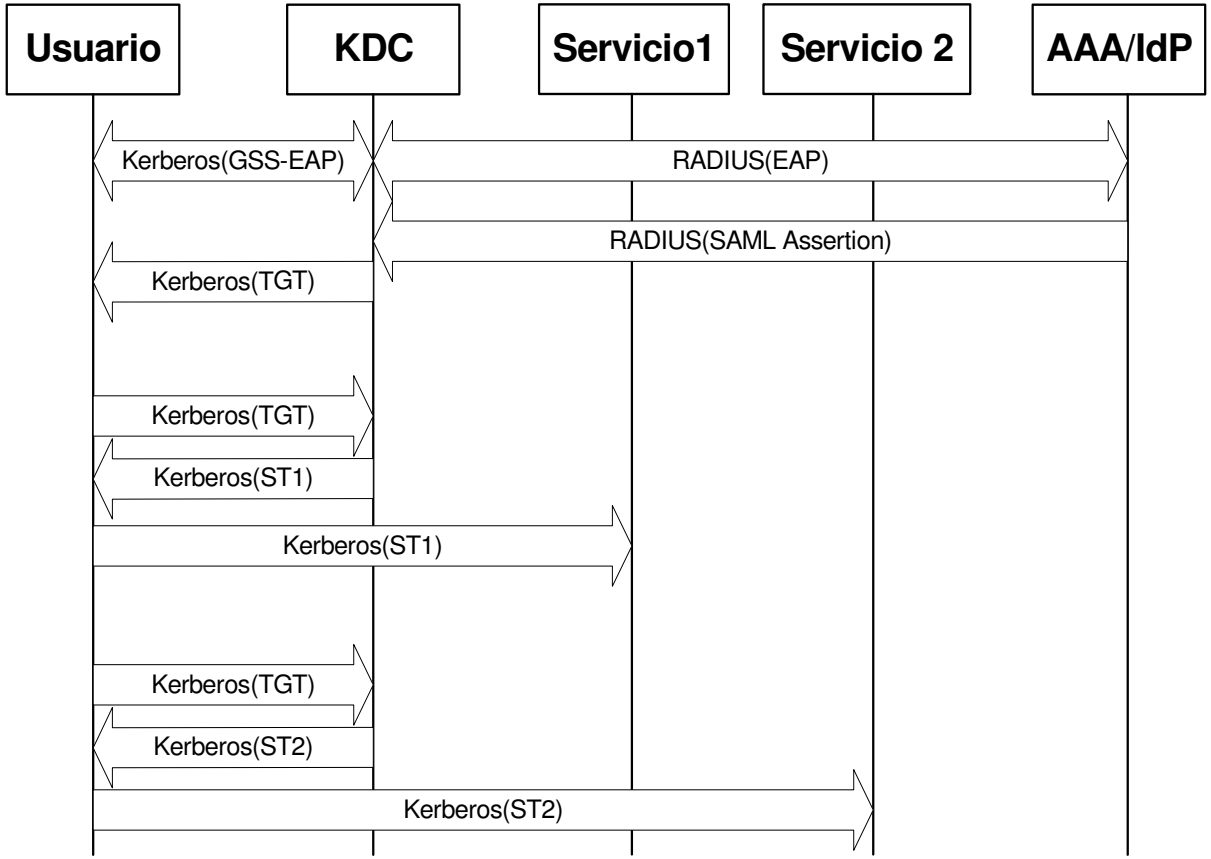
- Tecnologías en proceso de estandarización en el IETF WG ABFAB
  - GSS-EAP
    - Mecanismo GSS-API que usa EAP para realizar la autenticación
  - RADIUS-AAA
    - Definición del transporte de sentencias SAML sobre RADIUS
- Apoyo de otros grupos → RADEXT
  - RADIUS fragmentation
    - Soporte de fragmentación para paquetes RADIUS de más de 4KB

Moonshot & Kerberos

- Aspectos mejorables de la propuesta básica
  - Requiere cambios en los servicios para soportar GSS-EAP
  - No hay SSO → autenticación EAP completa en cada acceso a servicio
- Desde GÉANT se ha tratado de mejorar estos aspectos, integrando Kerberos en la federación AAA
  - Usuario consigue tickets Kerberos usando EAP para autenticarse con el dominio visitado
  - 3 alternativas:
    - Opción 1: Pre-autenticación Kerberos basada en GSS-EAP
    - Opción 2: Pre-autenticación Kerberos basda en el acceso a la red
    - Opción 3: Bootstraping Kerberos basado en PANA

Pre-autenticación Kerberos basada en GSS-EAP

- Escenario Moonshot puro
  - KDC → servicio
  - Tras autenticación, se presta el servicio → generar tickets para acceso a otros servicios

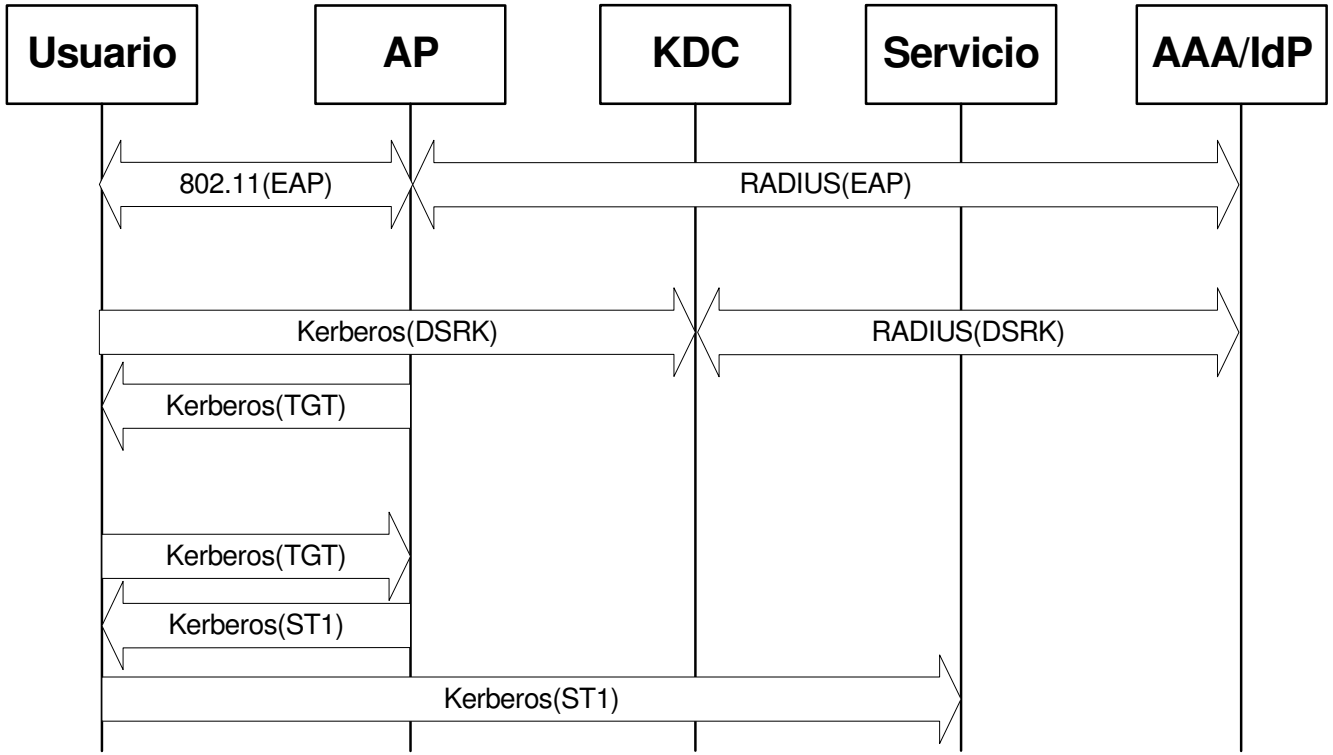


Pre-autenticación Kerberos basada en GSS-EAP

- Ventajas:
  - SSO basado en Kerberos
    - Menor número de autenticaciones EAP → 1 por dominio
  - Una gran cantidad de servicios soportan Kerberos hoy en día
    - Sólo hay que modificar el KDC, no los servicios
- Desventajas:
  - Kerberos no soporta GSS-API como mecanismo de autenticación
    - Necesita definir pre-autenticación Kerberos basada en GSS-API
    - draft-perez-krb-wg-gss-preauth-02
    - Implementación open-source disponible

Pre-autenticación Kerberos basada en el acceso a la red

- Optimización para reducir el número de autenticaciones EAP
  - Cuando el usuario ha sido autenticado para acceder a la red
  - Se aprovecha material criptográfico derivado para realizar la pre-autenticación (DSRK)



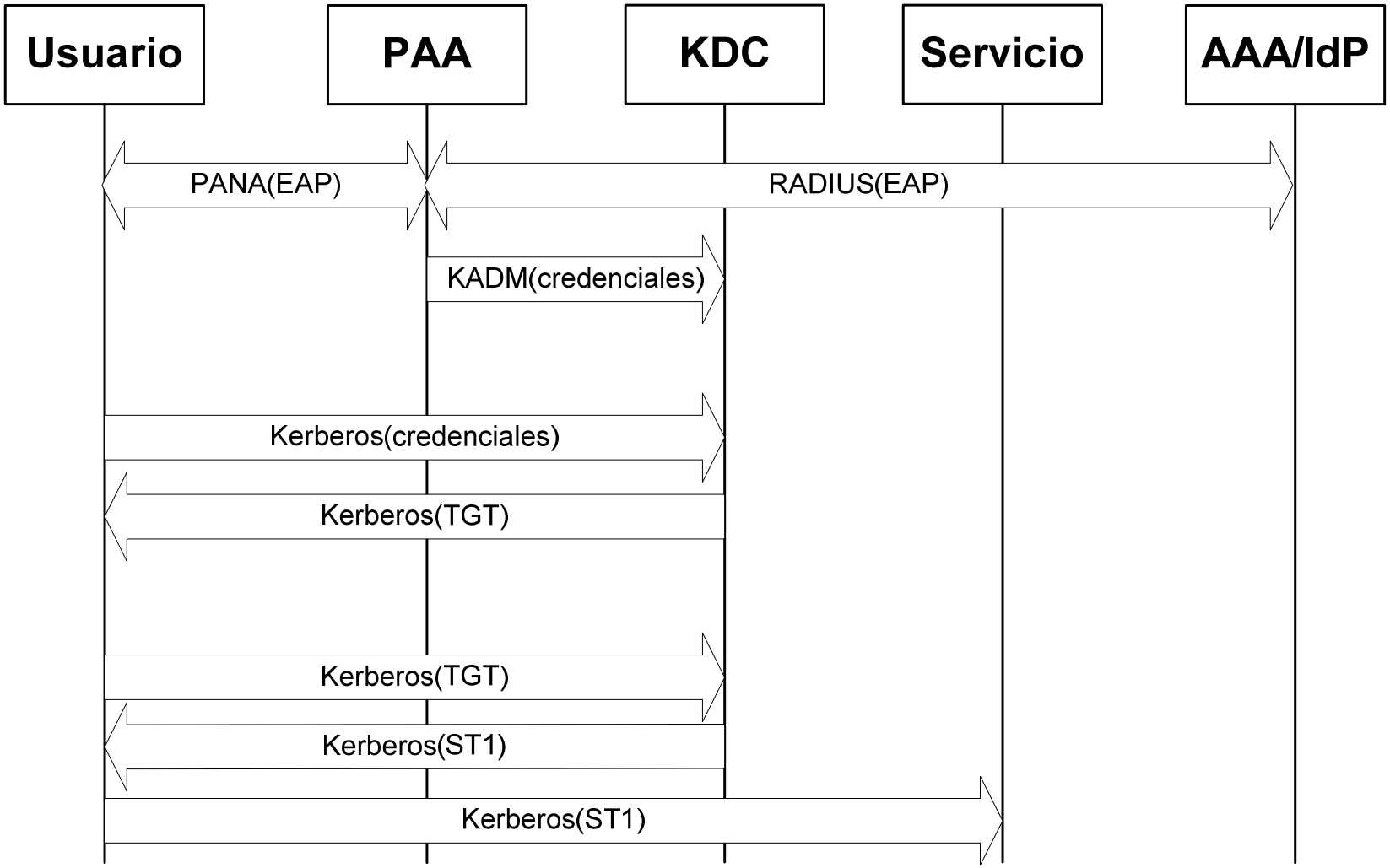
Pre-autenticación Kerberos basada en el acceso a la red

- Ventajas:
  - Se evita la autenticación EAP con el KDC
- Desventajas:
  - Requiere definir un mecanismo de pre-autenticación basado en material criptográfico EAP
    - Pérez-Méndez, A.; Pereñiguez-Garcia, F.; López, R. M. & Millán, G. L. A cross-layer SSO solution for federating access to kerberized services in the eduroam/DAMe network. IJIS. Sec., 2012, 11, 365-388

Boostrapping Kerberos basado en PANA

- Alternativa que evita la modificación de servicios y del KDC
- Requiere el despliegue de un nuevo elemento → PAA
  - El usuario se autentica con el PAA por medio de PANA y EAP
- Como resultado:
  - El usuario genera unas credenciales para Kerberos (i.e. password) del material criptográfico derivado de la autenticación EAP
  - El PAA deriva las mismas credenciales y las instala en el KDC
- El usuario puede ahora realizar una autenticación Kerberos completamente estándar
- Ventajas:
  - Ni el KDC ni los servicios requieren modificaciones
- Desventajas:
  - Requiere el despliegue de un nuevo elemento

Boostrapping Kerberos basado en PANA



Muchas gracias por su atención

¿Alguna pregunta?