Autenticación y autorización en federaciones de identidad, de la red a los servicios de alto nivel

Gabriel López Millán (UMU)

Agenda

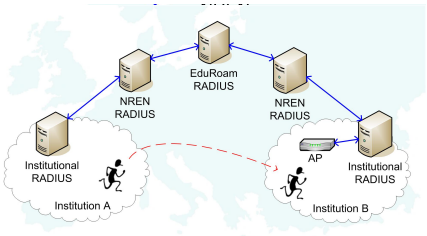
- eduroam
- DAMe
- Moonshot/ABFB
- KRB-Moonshot

III Foro de Movilidad y II Foro de Identidad de RedIRIS

UNIVERSIDAD DE MURCIA

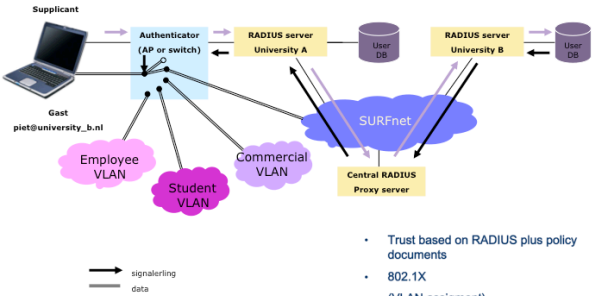
eduroam

- Servicio de roaming inter-institucional basado en la arquitectura 802.1X y una infraestructura AAA jerárquica basada en servidores RADIUS
- Servidor(es) de alto nivel proporcionados por TERENA
  - Formada por la gran mayoría de los National Research and Educational Networks (NREN's) europeos
  - Desplegado también en EEUU, Canada y Asia-Oceanía
  - Cada institución que desea conectarse a eduroam conecta su propio servidor RADIUS a su NREN nacional



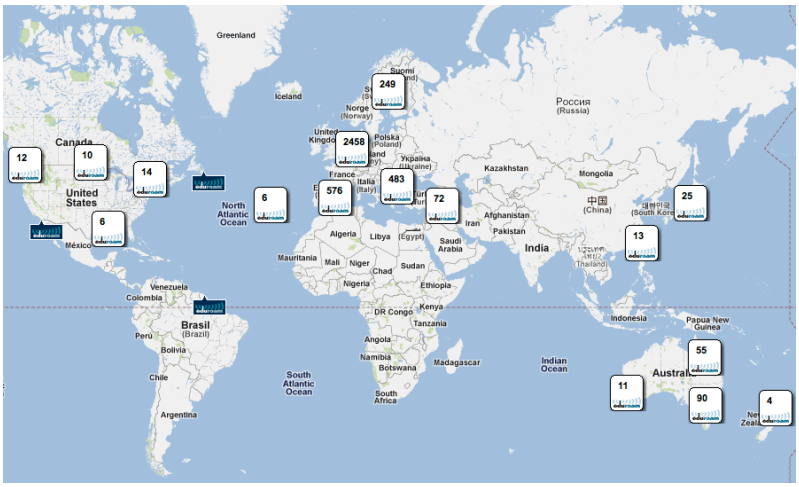
eduroam - arquitectura

- Seguridad basada en 802.1X (or web-based redirect)
  - Diferentes mecanismos de autenticación
  - Autenticación mutua (PEAP, TTLS, TLS)
  - Protección de credenciales
  - Integración con la asignación de VLANs específicas
    - Normalmente para usuarios "locales", no se discrimina entre usuarios remotos
- Roaming se basa en la confianza delegada en la arquitectura RADIUS



- Trust based on RADIUS plus policy documents
- 802.1X
- (VLAN assigment)

The eduroam service in the world



eduroam

- Control de acceso basado en la autenticación del usuario: nombre de usuario (email) y contraseña
- Muy limitado
- Organizaciones no pueden diferenciar el tipo de usuario (normalmente, el externo)
  - Rol: estudiante, profesor, investigador
  - Edad
  - Idioma
  - ….
- Ofrecer servicios diferenciados
  - VLANs por rol
  - QoS
  - Contenidos adaptados
  - …

Jugando con la autorización: DAMe

(Deploying Authorization Mechanisms for eduroam)

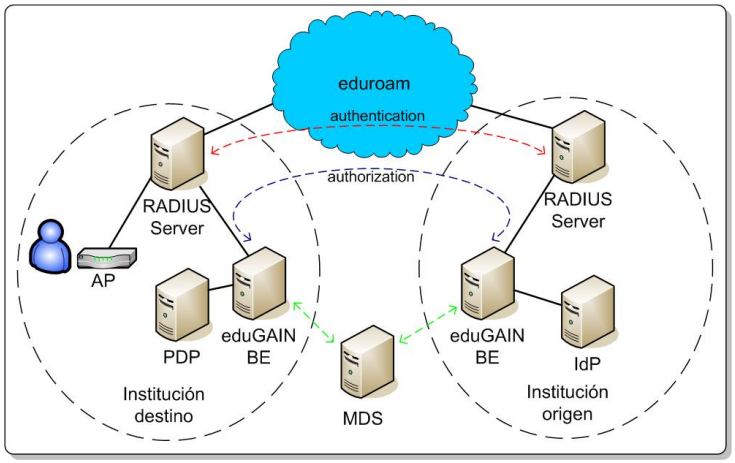
Objetivos

- Una vez autenticado al usuario para el acceso a la red obtener información adicional (atributos) desde su organización origen para ofrecer servicios diferenciados

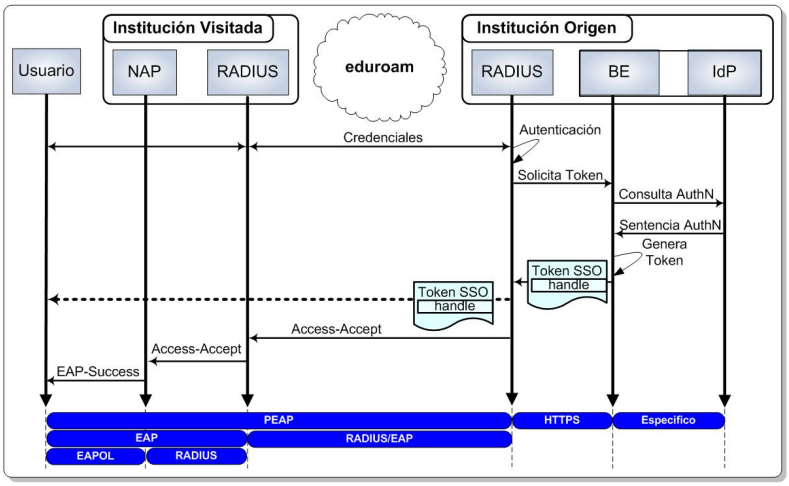
DAMe: Arquitectura

- Movilidad de red basada en eduroam
- AAI para gestionar la identidad y atributos de los usuarios
  - Proveedor de Identidad(IdP) en cada institución
  - Encargado de controlar el acceso a los atributos de los usuarios
- Protocolo basado en SAML como lenguaje para representar la información de los usuarios
  - Sobre autenticación
  - Sobre atributos
- Publicación de metadatos (localización de idPs) en MDS
  - Basado en eduGAIN
- Sistema de autorización flexible y genérico
  - Puede ser usado en la red o en diferentes servicios de alto nivel
  - Para facilitar el intercambio de atributos, es habitual definir un esquema común como eduPerson/SCHAC
  - Sistema de control de acceso final basado en políticas XACML
- Ofrece además un servicio de SSO "cross-layer"

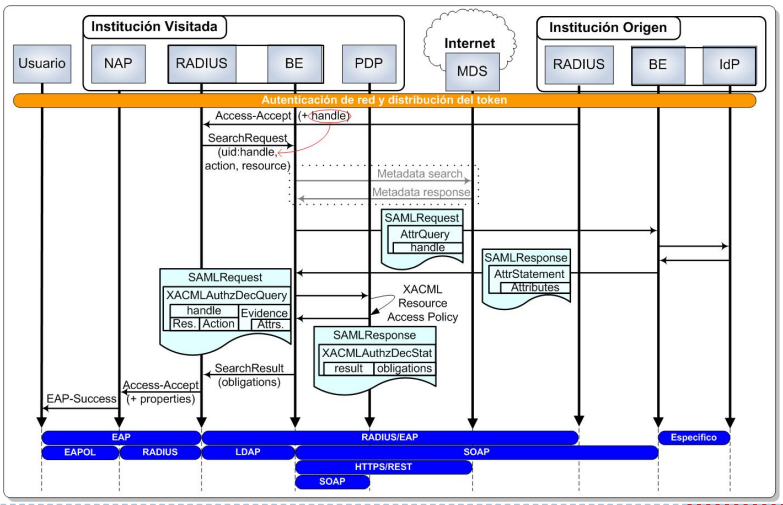
Arquitectura



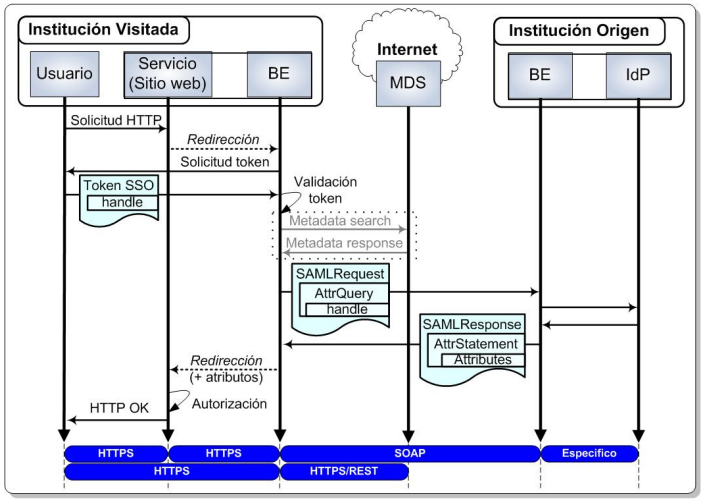
Autenticación de Red



Perfiles de Autorización – Red (y II)

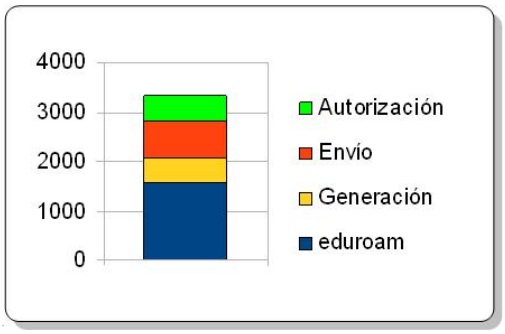


Perfiles de Autorización – Web SSO



Rendimiento

- Pruebas realizadas sobre los organizaciones de eduroam
  - Media eduroam: 1568 ms
  - eduroam+distribución token 2817 ms
  - Autenticación+ Autorización de red: 3376 ms (con BE's independientes)



DAMe

- Centrado en el acceso a la red
- Prototipo de aplicación en servicios Web sin estandarizar
- Soluciones existentes para los servicios Web ya funcionando
  - PAPI
  - OpenID
  - Shibboleth
  - CAS
  - Oauth
  - …
- ¿Por qué no ofrecer SSO a cualquier tipo de servicio de modo homogéneo?
- ¿Por qué no aprovechar el SSO cross-layer?

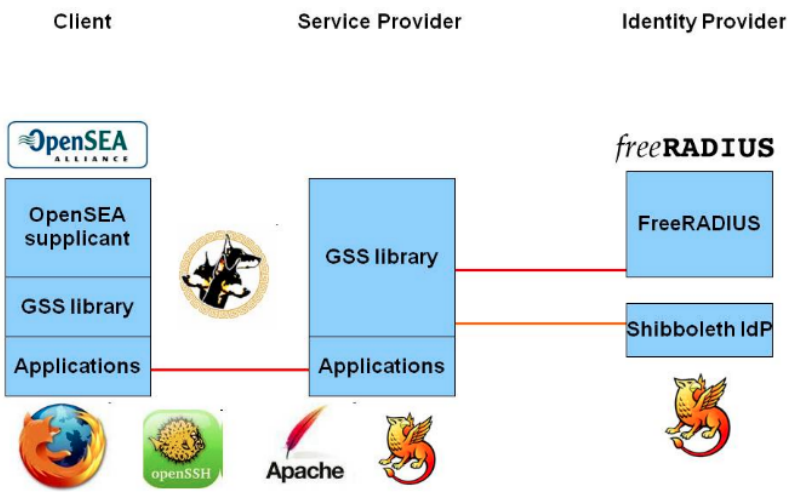
Moonshot/ABFAB

(Application Bridging for Federated Access Beyond web IETF WG)

Moonshot/ABFAB

- Ofrecer acceso federado a servicios más allá del web
  - SSH, SMTP, FTP, XMPP, ….
  - No tiene en cuenta el acceso a la red
  - No abarca el SSO cross-layer
- Moonshot
  - Integración EAP sobre GSS-API para autenticación en servicios de aplicación
  - Integración AAA para autenticación y SAML para autorización
- ABFAB (Application Bridging for Federated Access Beyond web) IETF WG
  - Estandarización de las tecnologías requeridas para Moonshot
    - GSS-EAP, RADIUS-SAML,…

Moonshot/ABFAB



ABFAB – Propuestas de estandarización

- Arquitectura general
  - draft-ietf-abfab-arch-02
- Encapsular EAP sobre GSS-API
  - draft-ietf-abfab-gss-eap-02
- Encapsular sentencias SAML sobre AAA
  - draft-ietf-abfab-aaa-saml-01
- Definir casos de uso
  - draft-ietf-abfab-usecases-01
- Establecimiento de confianza basado en KNP (sin infraestructuras PKI)
  - draft-mrw-abfab-multihop-fed-01

Moonshot/ABFAB

- Problemas
  - Todo servicio debe hablar GSS-EAP para autenticación
  - Todo servicio debe entender SAML para autorización
    - Hay que adaptar todos los servicios
  - No define una solución de SSO
  - No se tiene en cuenta el control de acceso basado en XACML

Moonshot basado en Kerberos

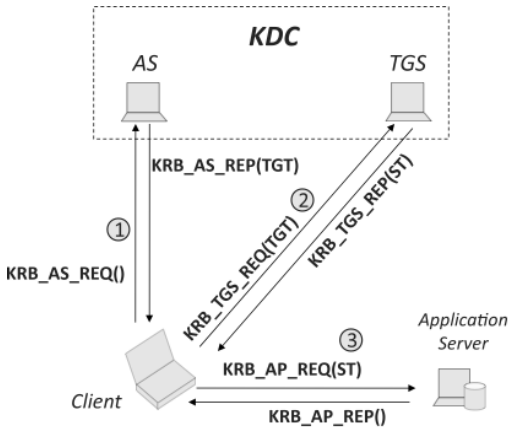
Introducción

- Infraestructuras Kerberos → SSO en el acceso a servicios dentro de una organización
  - Soporte en sistemas operativos (Windows, Linux, OSX…) y aplicaciones (FTP, SSH…)
  - Despliegues federados (*cross-realm)* son inusuales
- Infraestructuras AAA → control de acceso en redes federadas
  - Uso de EAP para autenticación
    - Ej. Eduroam
  - Muy extendidas

Introducción

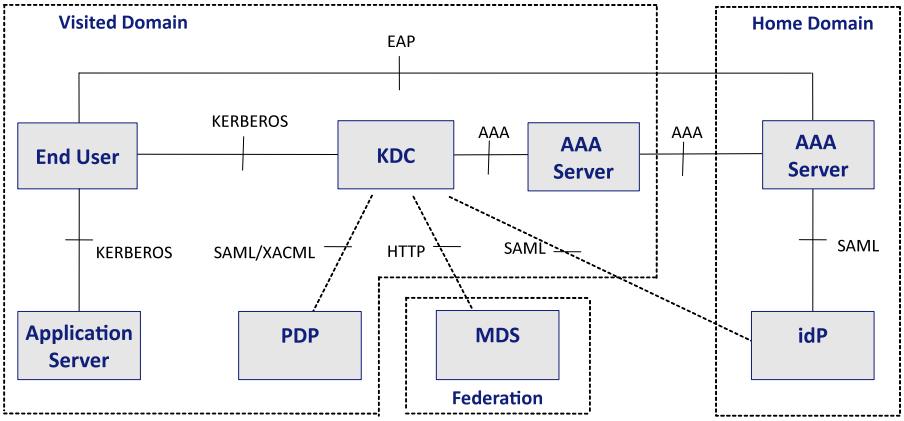
- Objetivo 1 → integrar infraestructuras AAA federadas con el control de acceso a servicios basado en Kerberos
  - Permite autenticación de usuarios pertenecientes a otros dominios en la federación
  - Evita despliegue de Kerberos *cross-realm*
- Objetivo 2 → proporcionar gestión de la autorización al proceso
  - Permite integrar información de identidad a la decisión de control de acceso a un servicio en el KDC
- Objetivo 3 → conseguir SSO cross-layer

Kerberos

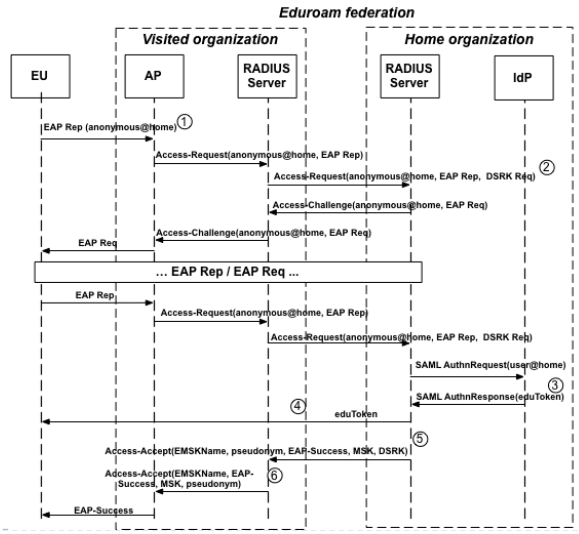


III Foro de Movilidad y II Foro de Identidad de RedIRIS
UNIVERSIDAD DE MURCIA

Arquitectura propuesta

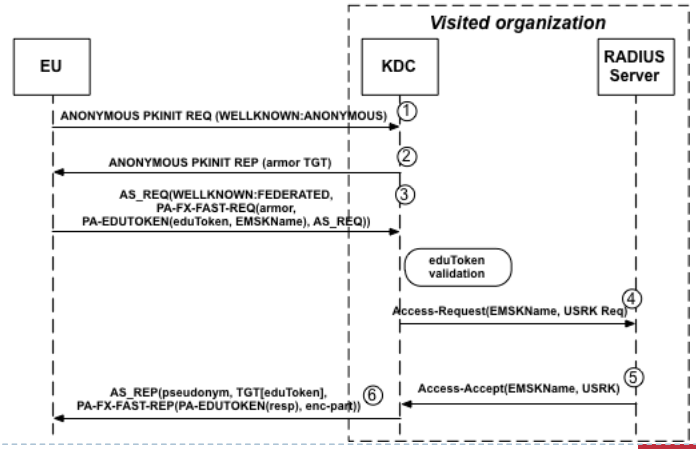


Fase de autenticación en el acceso a red

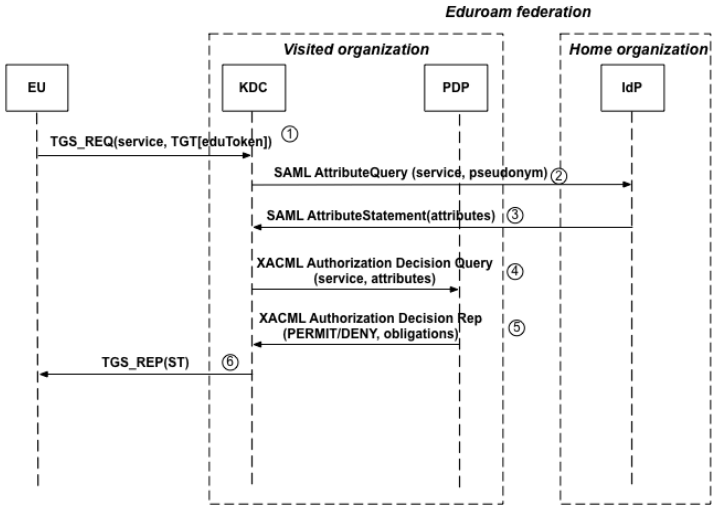


Fase de autenticación acceso al servicio

- Obtención de ticket TGT para el acceso a servicios



Fase de autorización



Moonshot basado en Kerberos

- No hace falta modificar los servicios de aplicación
  - Todos soportan Kerberos
- La gestión de decisión de autorización se lleva al KDC
  - Transparente para el servicio
  - Centralizado
- No hace falta desplegar KRB cross-realm
  - Se delega en la infraestructura AAA
- Se proporciona SSO cross-layer
  - Mediante el edutoken

Conclusiones

- eduroam como infraestructura de roaming desplegada a nivel mundial
  - escenario idóneo
- Interés en la toma de decisiones basada en atributos del usuario (itinerante o local)
  - Ofrecer servicios diferenciados
- Llevar la federación de servicios más allá del web
  - Interés del IETF
- Pero no a cualquier precio
  - KRB ofrece una solución válida
- Estandarizar eduToken para servicios Web
- Añadir más tipos de servicios: VoIP?

- Preguntas?


¿Quien eres tú?
Desde ahora yo seré tú y nadie más salvo nosotros dos sabremos la verdad...
Mblog