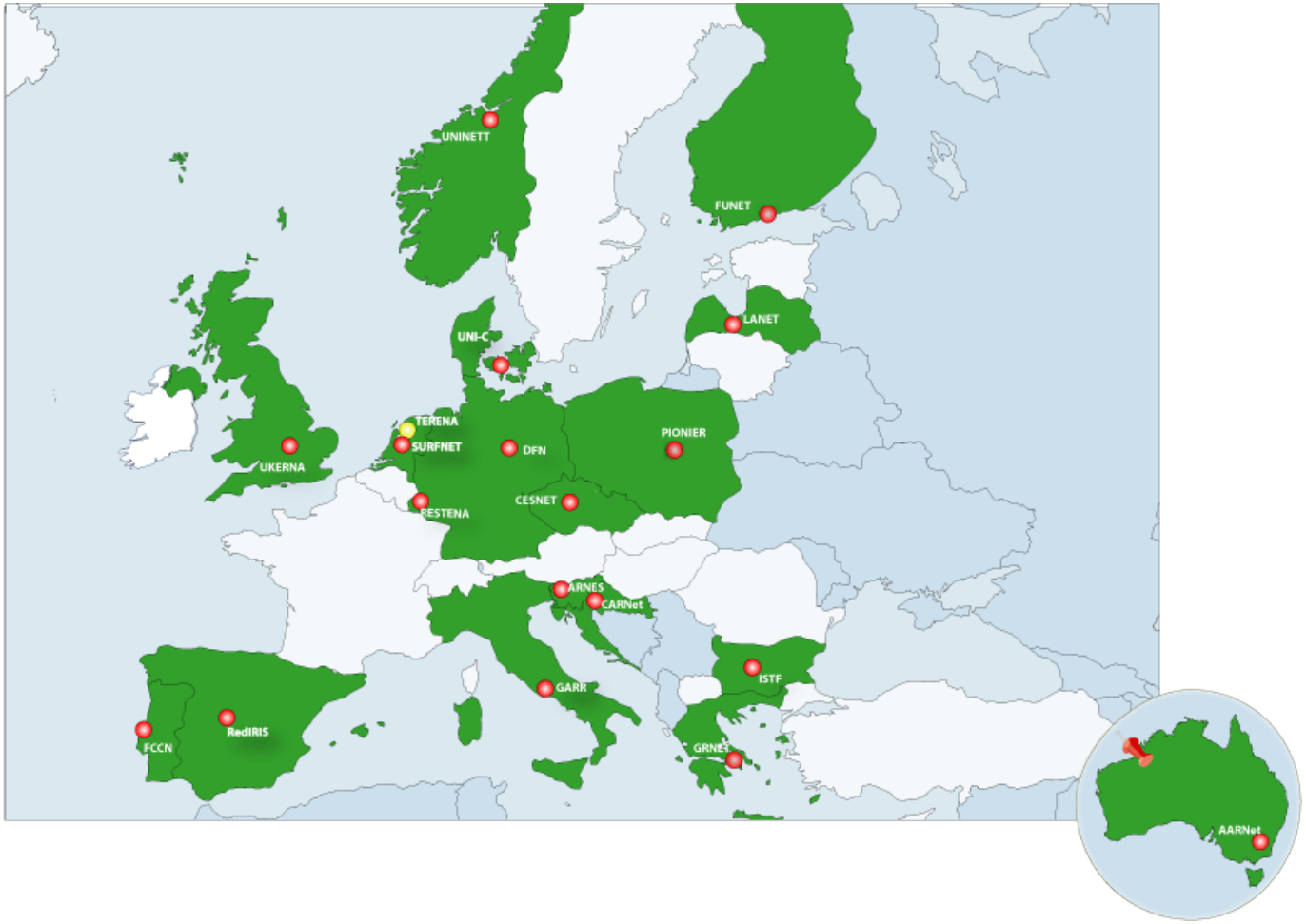
Espacio común de movilidad

eduroam a nivel internacional

eduroam internacional

- Bulgaria
- Croatia
- Czech Republic
- Denmark
- Finland
- Germany
- Greece
- Italy
- Latvia
- Luxembourg
- the Netherlands
- Norway
- Poland
- Portugal
- Slovenia
- Spain
- UK

eduroam internacional

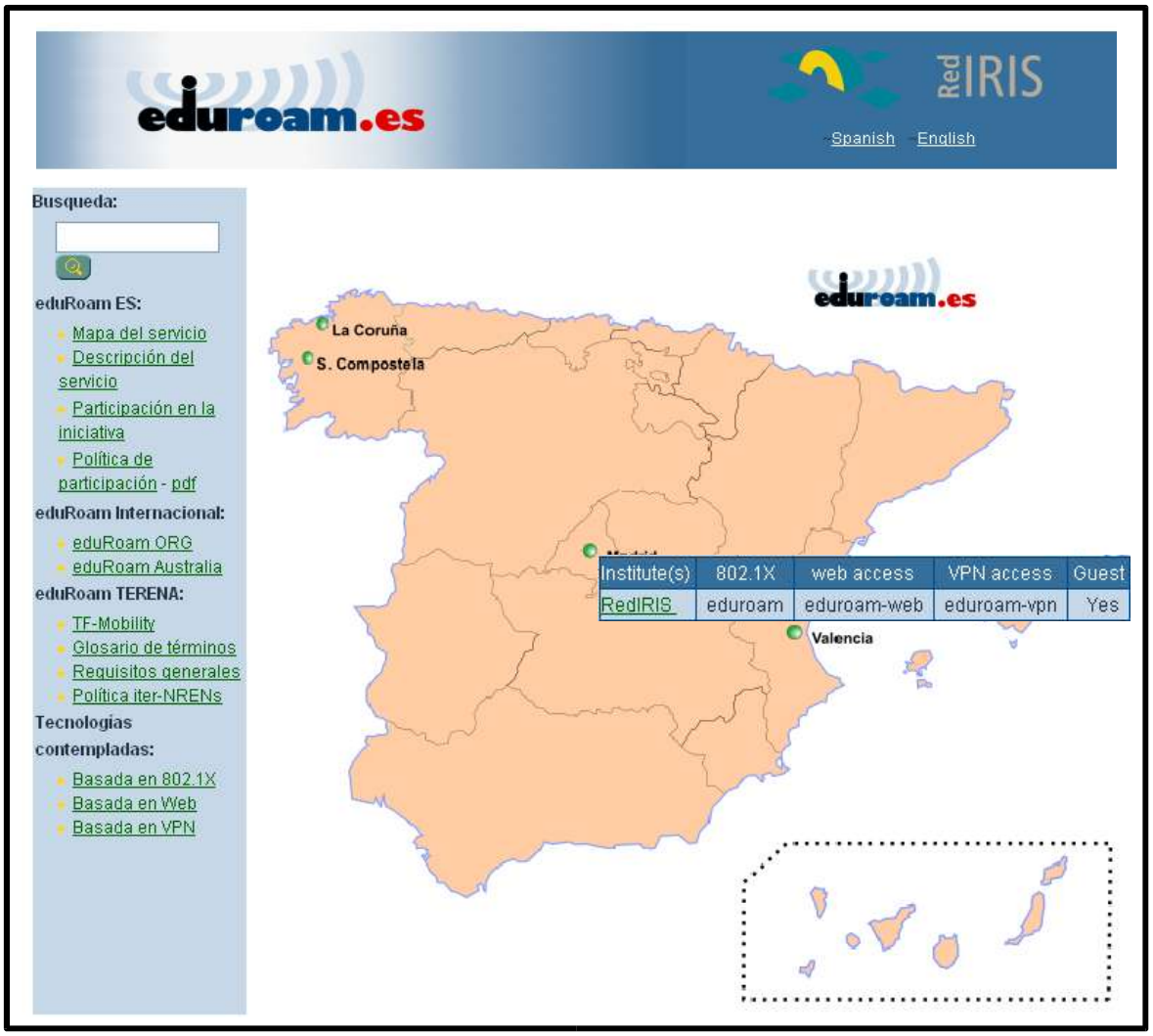


JRA5 - roaming

- **Proyecto englobado en Geant2 para la creación de una infraestructura de AA y roaming.**
- **Evaluación de consecuencia jurídicas en la política de uso**
  - Accesible en el grupo de movilidad de terena (TF-Mobility)
- **A punto de cerrar el documento de especificación de requisitos**

eduroam a nivel nacional

Nueva web eduroam.es



Colaboración red.es - CRUE

- **Objetivo: Apoyar la implementación de infraestructura inalámbrica a nivel universitario**
- **Comité técnico de evaluación**
  - Desarrollo de las bases técnicas de la convocatoria
- **Soluciones alineadas con "eduroam.es"**
  - Técnico
  - Política
  - Gestión
  - Infraestructura informativa

Política de uso

- **Usuarios con derecho de acceso**
  - Perfil de usuarios?
- **Condiciones técnicas mínimas**
- **Registro y seguimiento**
- **Información y soporte**
- **Servicios mínimos a prestar**
  - Conexión a Internet
  - Puertos abiertos
  - …

Aspectos WIFI

Encriptación WIFI

- **WEP**
  - Alg RC4: 40 – 128 bits
  - IVs inicializados a 0 al inicializar la tarjeta
  - Clave estática compartida a nivel de cliente
  - http://www.eduroam.es/Attack-to-Break-WEP.htm
- **TKIP**
  - Alg RC4 128 bits
  - Clave dinámica distribuida por el servidor de autenticación
  - Cambio de clave por paquete PPK
  - MIC (Michael Integrity Check)
- **AES-CCMP**
  - Claves de 128 bit
  - CBC-MAC (Cipher Block Chaining Message Authentication Code)

Estándares WIFI

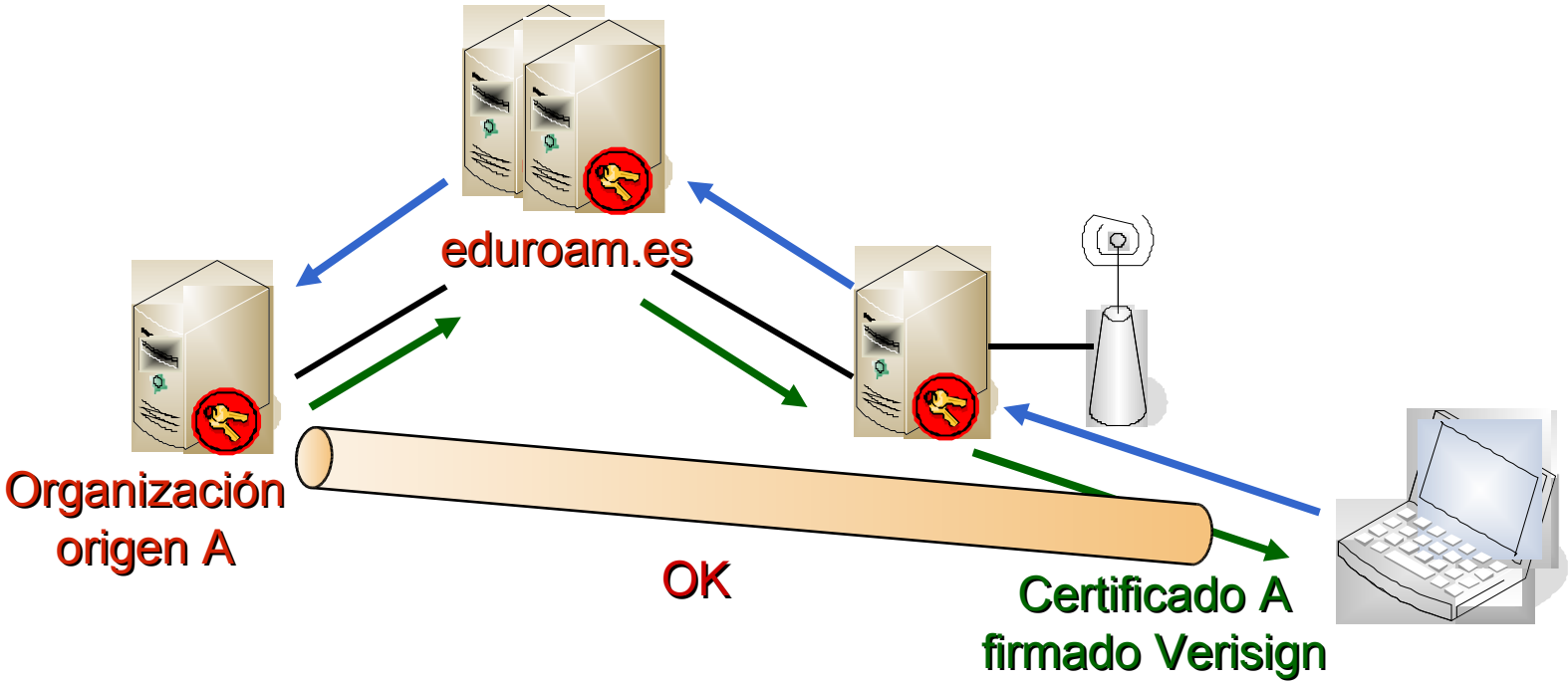
- **WPA**
  - Encriptación
    - TKIP(MIC,PPK,clave dinámica)
    - Broadcast para rotación de clave
  - Autenticación
    - PSK (ámbito personal)
    - EAP 802.1X
- **WAP2**
  - Compatible WPA
  - Encriptación AES-CCMP

SSIDs

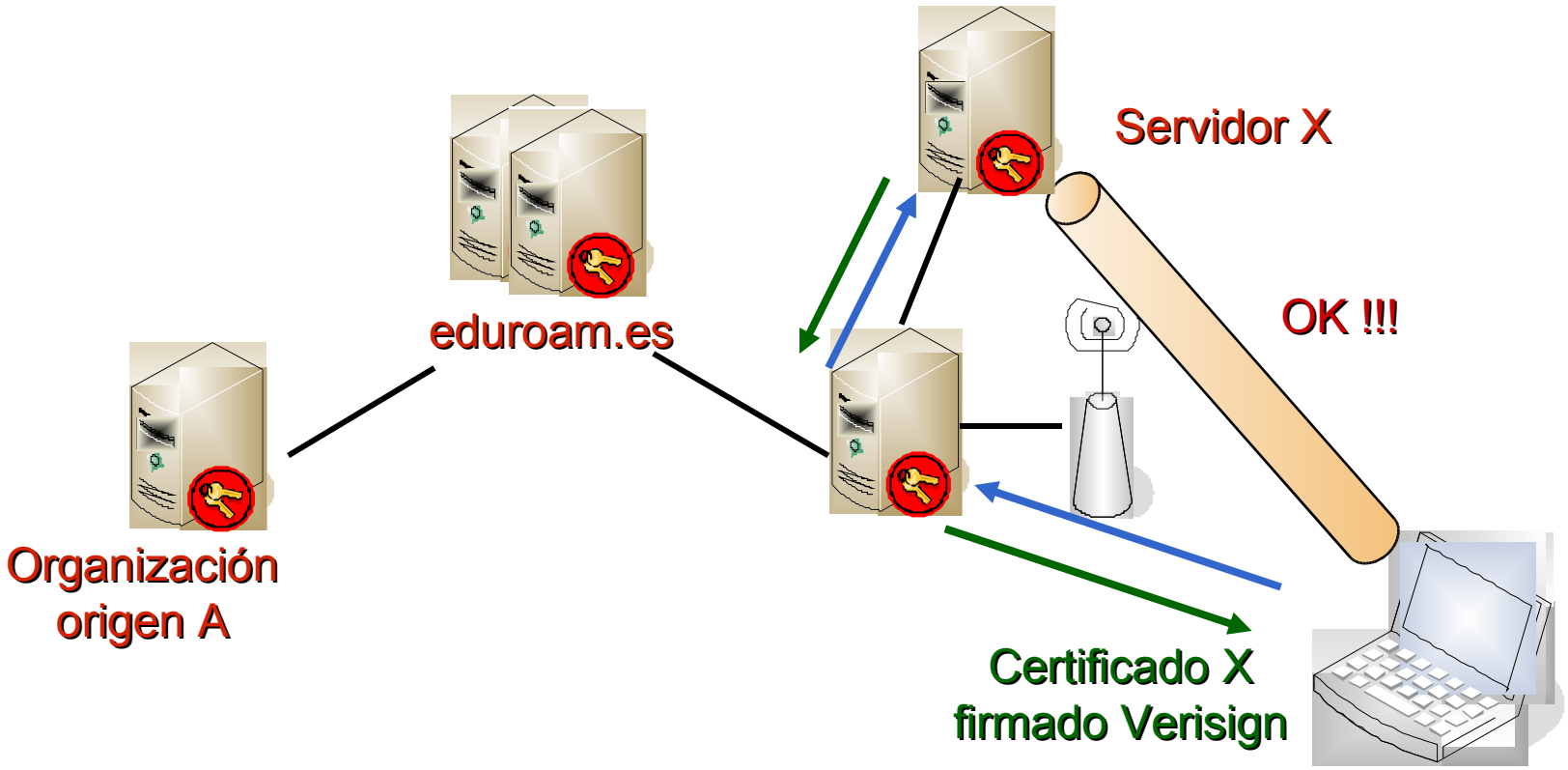
- **Qué SSIDs utilizar**
  - “eduroam”
  - Si es posible técnicamente y beneficia a la de la comunidad, es deseable tener más SSIDs tipo: eduroam-….:
    - eduroam-wep
    - eduroam-aes
    - …
  - Se debe fomentar la utilización del SSID eduroam que corresponderá con el cifrado considerado por la organización.

Ataque a EAP-TTLS

- Ataque a EAP-TTLS
  - http://www.eduroam.es/eap-ttls-attack.pdf



Ataque a EAP-TTLS (II)



Ataque EAP-TTLS: posibles soluciones

- **Certificado autofirmado**
  - Autorizar en el cliente sólo a esa CA
- **Incluir nombre de servidor en los certificados "CN"**
  - Definir en el cliente el nombre del servidor a conectar

Curiosidades

- **Freeradius: 1.0.2**
  - Parche para añadir regex a los realms

```
realm .uni.es {
        regex           = "^.*\.uni\.es$"
    ...
}
```

- **MBSSIDs**
  - Cisco IOS Release 12.3(4)JA
  - Para interfaces 802.11a o 802.11g

"Number of supported simultaneous BSSID on radio_interface: 8"

Preguntas
Dudas
Comentarios
...