



perfSONAR

AAI for network-oriented services

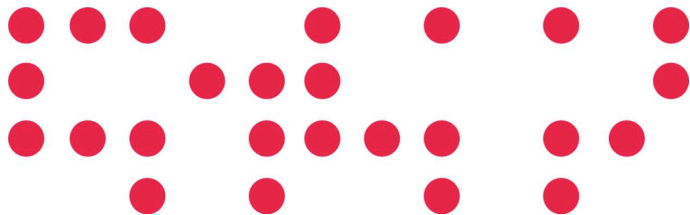
Cándido Rodríguez

candido.rodriguez@rediris.es

1. Scenario of perfSONAR

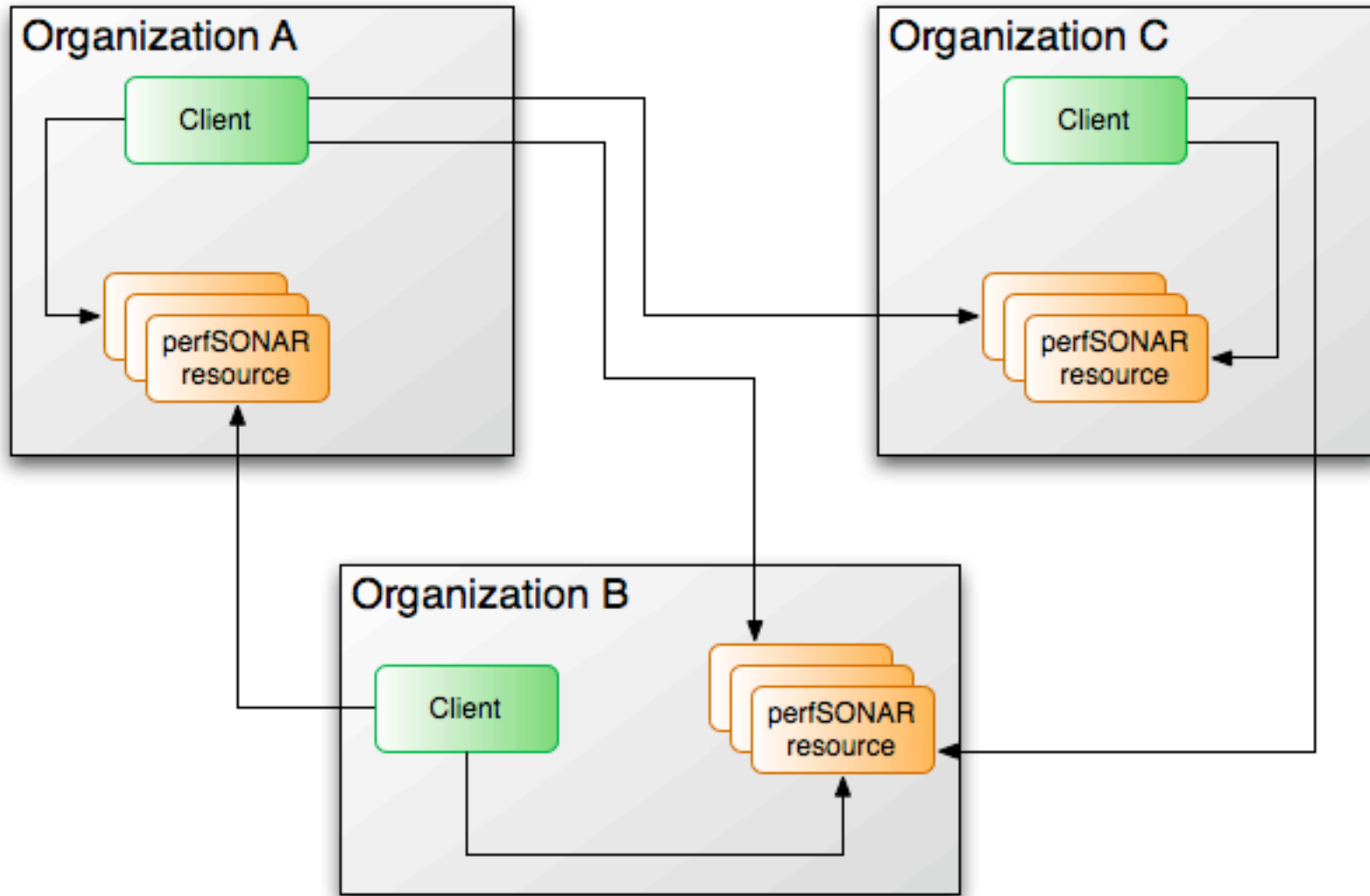
2. Using eduGAIN

3. Some comments



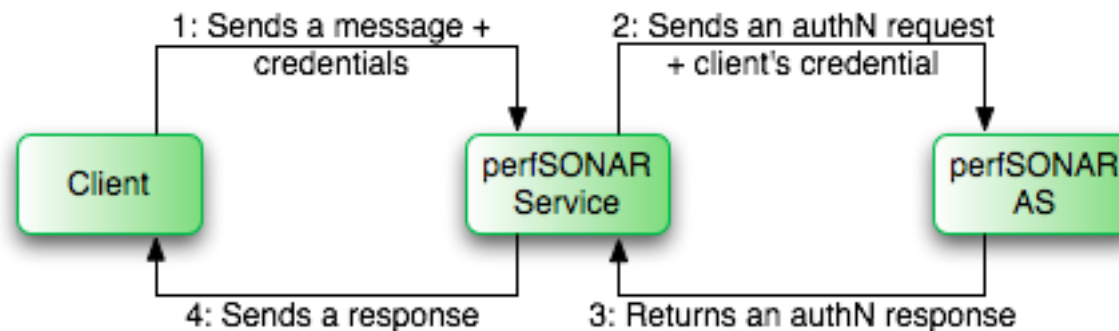
- **What is perfSONAR?**
 - Multi-Domain Monitoring (MDM) tool
 - Generic solution for network-oriented services
 - Protocol based on SOAP messages and following the Open Grid Forum Network Monitoring Working Group (OGF NM-WG)
 - Partners: GÉANT2, Internet2, ESnet and RNP
- **Building the AAI for perfSONAR**
 - An Authentication and authorization service
 - The AuthN part for the MDM perfSONAR 3.0 (**Now!**)
 - The AuthR part for the MDM perfSONAR 4.0 (In 6 months)
 - It uses eduGAIN
 - Best solution for a multi-domain scenario

- Initial scenario



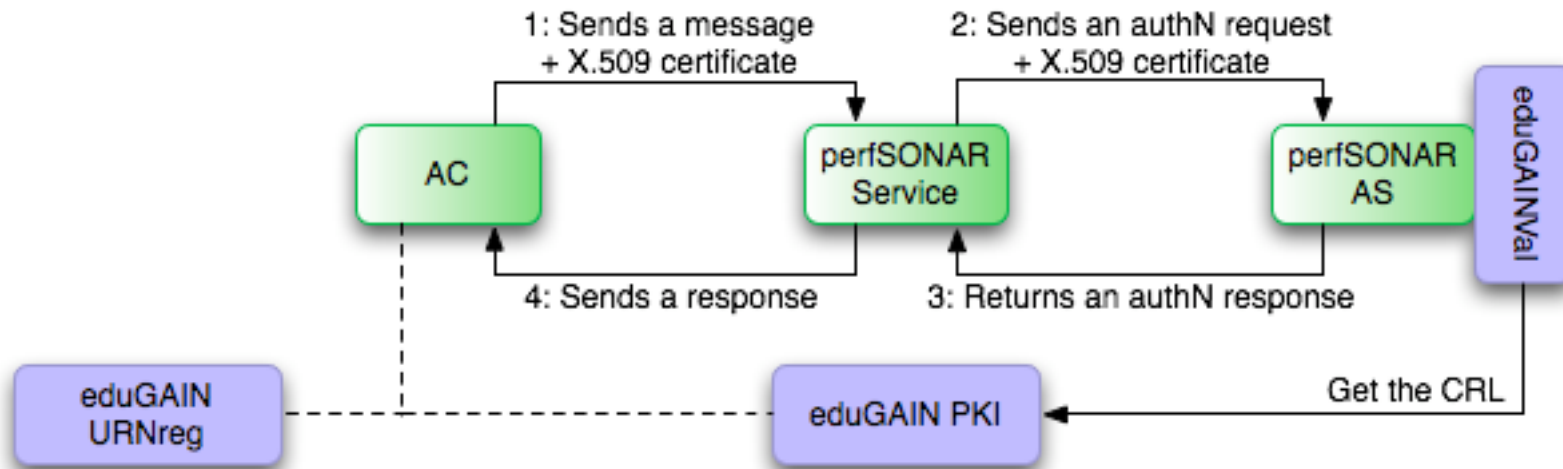
- A complex scenario
 - perfSONAR resources (pSR) in different networks
 - Services with an specific activity: measurement, topology, ...
 - Java
 - Perl
 - Python
 - Clients
 - Applications analyzing and showing data from pSRs
 - Perl scripts
 - Java Applications
 - Java Applications distributed under Java Web Start
 - PHP web application

- Roles from the point of view of AA
 - Clients
 - Send a security token representing who/which are
 - Services
 - Resources send authN requests to an AS if they want
 - Authentication Service
 - Another perfSONAR service
 - Processes authN requests and sends authN responses



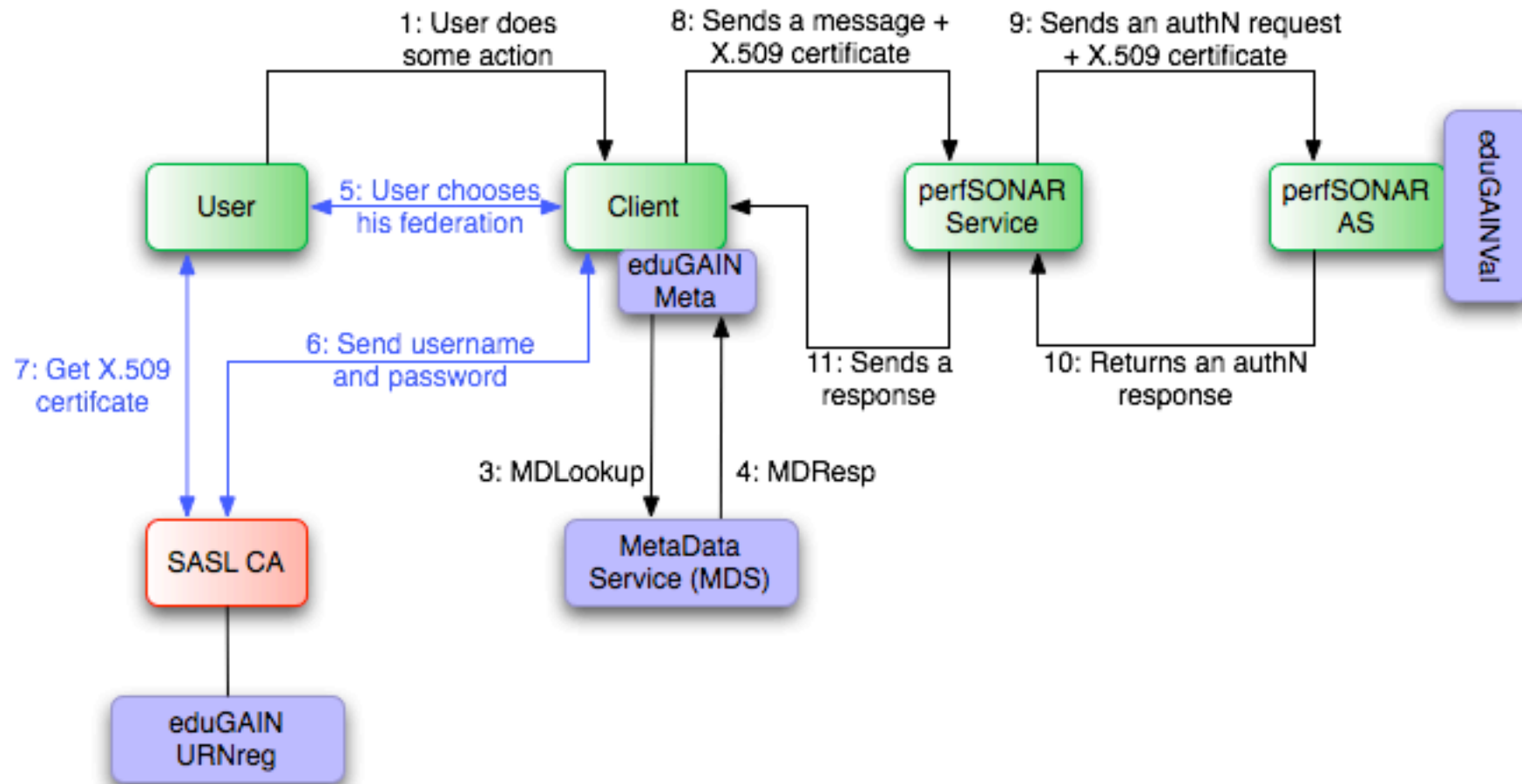
- **Transmission of credentials**
 - Clients send security tokens representing themselves
 - Web Service Security standard
- **Different clients - different profiles**
 - Without human interaction
 - Scripts
 - **Automated Client (AC) profile**
 - With human interaction
 - Web-based applications
 - **Client in a Web containEr (WE) profile**
 - Non web-based applications
 - **User behind a Client (UbC) profile**

Scenario of perfSONAR: AC profile



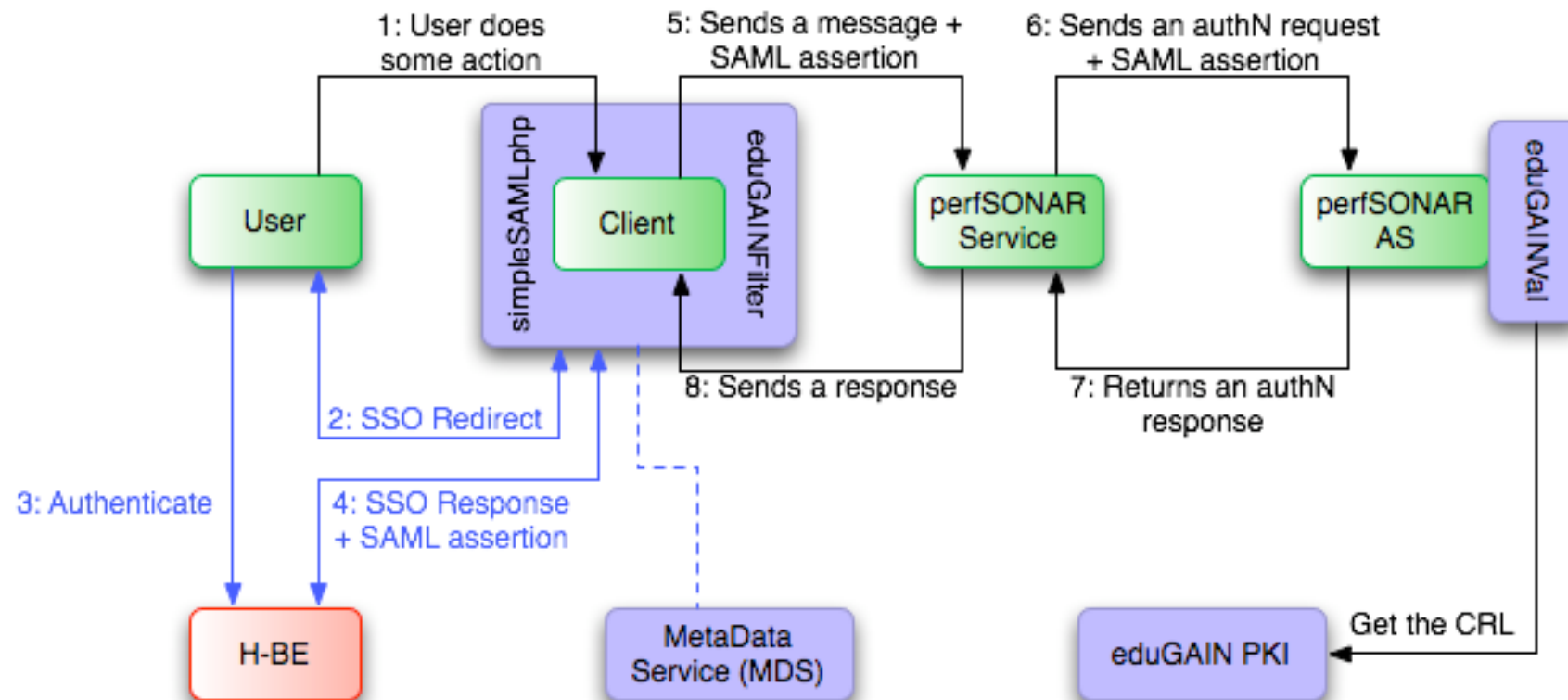
- Unique and non-transferable ID for each client
 - URN obtained from eduGAIN URN registry service
 - Private and public key valid in the eduGAIN trust model
 - Subject Alternative Name of the cert contains the URN
 - Obtained from eduGAIN PKI
- Security Token is based on the X.509 certificate

Scenario of perfSONAR: UbC profile



- A similar case than AC but using an online CA for getting the certificate
 - SASL CA is used for this

Scenario of perfSONAR: WE profile

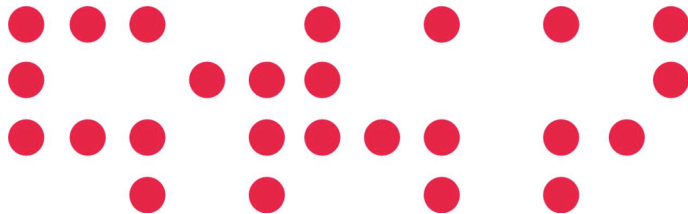


- Uses the eduGAIN webSSO profile
- SAML assertions contain user's credentials
- Clients must have a pair of keys valid in the eduGAIN trust model
- Security Token is based on SAML assertions

1. Scenario of perfSONAR

2. Using eduGAIN

3. Some comments

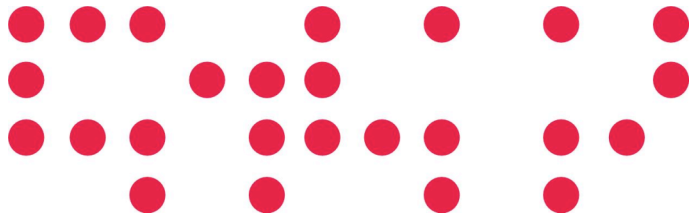


- **What does eduGAIN offer perfSONAR?**
 - An unified framework of digital identity
 - URN registry service
 - PKI service
 - Neutral area of identity providers and messages
 - Shibboleth, PAPI, FEIDE, A-Select, ...
 - MetaData Service
 - GÉANT Identity Provider (GIdP) for “homeless”
 - Java-based libraries for interacting with eduGAIN components
 - eduGAINMeta, eduGAINVal, ...
- **What does NOT eduGAIN offer perfSONAR?**
 - An Authentication and Authorization Service

1. Scenario of perfSONAR

2. Using eduGAIN

3. Some comments



- **The WE profile cannot be implemented**
 - perfSONAR Java services are based on Axis 1.4
 - Axis implements DOM v2 and openSAML DOM v3
 - Signed XML message by OpenSAML is not the same that Axis sends
 - There is a workaround
 - Using the X.509 certificate profile of WS-SEC
 - SAML assertion -> BLOB in base 64 -> Binary security token
- **UbC profile is not a good solution (I/II)**
 - User's credential is a valid certificate in the eduGAIN trust model
 - In eduGAIN, certificates was though for components
 - Contains a registered URN
 - This model is quite odd for users

- **UbC profile is not a good solution (II/II)**
 - SASL CA
 - An online CA without support
 - Would we install it?
 - If it is not installed in a federation, perfSONAR cannot use that federation
 - We're "condemned" to use only GIdP
 - Not using an standard protocol of communication, like XKML
- **A new SAML-based profile would be a solution**
 - Security tokens are based on SAML assertions



MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

red.es



MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

red.es

Edificio CICA, Campus Universitario
Avenida Reina Mercedes s/n
41012 Sevilla. España

Tel.: 95 505 66 00
Fax: 95 505 66
www.red.es
www.rediris.es

