Aretusa

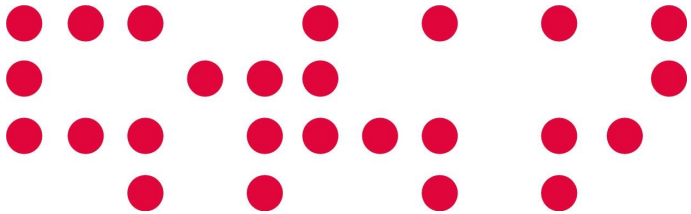
Sistema de reputación para BitTorrent

Jornadas Técnicas RedIRIS

21 – 23 de noviembre 2007

Jaime Perez <jaime.perez@rediris.es>

1. BitTorrent y el “free-riding”
2. Solución propuesta
3. Implementación



Free-riding

- Problema común a aplicaciones p2p.
- Un cliente puede descargar archivos sin subir nada.
- Comportamiento egoista. Consume ancho de banda y perjudica a todos.

Free-riding en BitTorrent

- BitTorrent (a pesar de Bram Cohen) no está exento. Sistema de incentivos.
- Relacionado con teoría de juegos.
- Demostraciones prácticas:
  - BitThief
  - http://dcg.ethz.ch/projects/bitthief

Free-riding

- ¿Por qué evitarlo?
  - Consume recursos sin generar beneficios.
  - Una mayor eficiencia atraerá a más usuarios.
  - A más usuarios y mayor uso, beneficio de todos.
- ¿Cómo evitarlo?
  - Identificar a los pares de forma unívoca en la red, de forma permanente.
  - Asociar a los pares una reputación acorde a su comportamiento en la red.

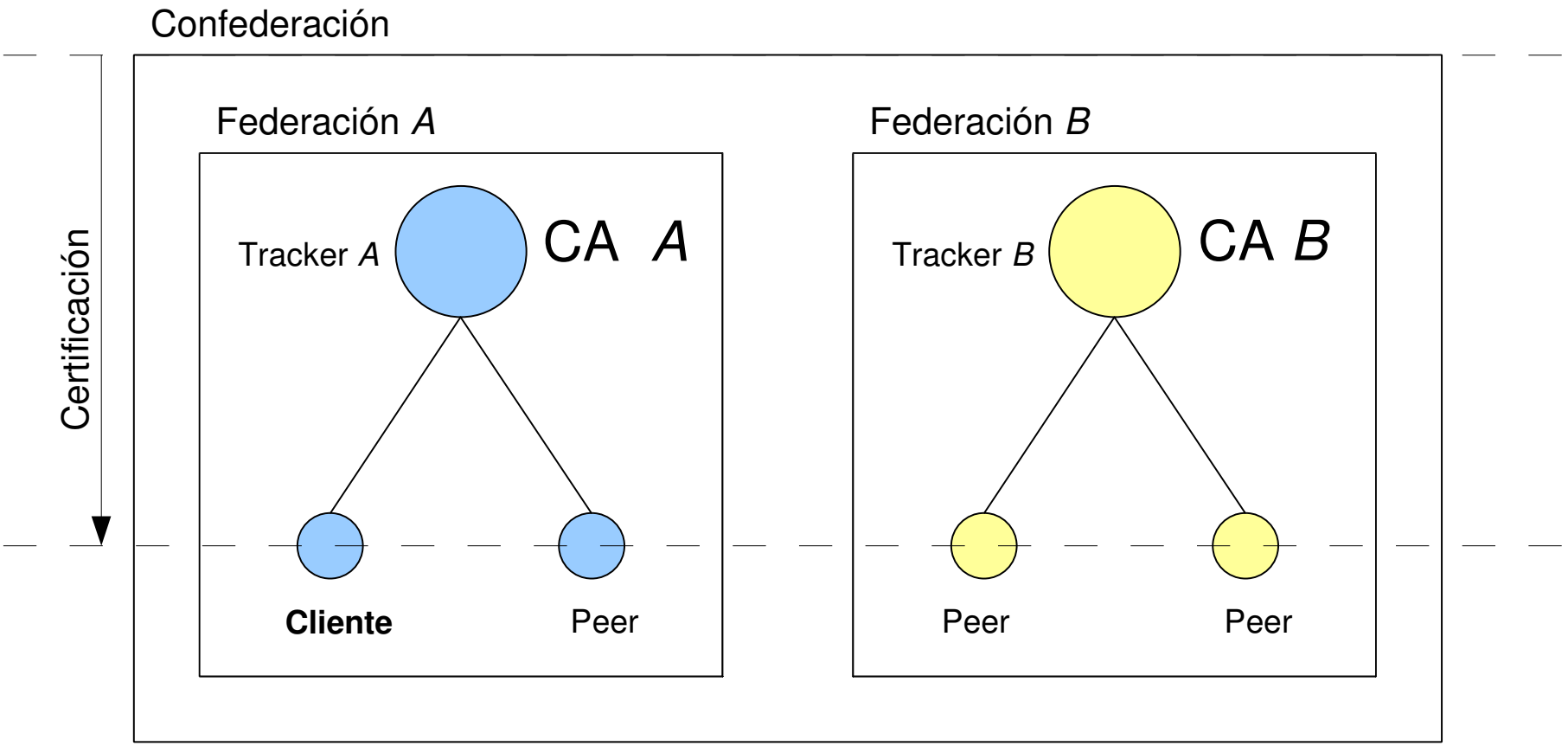
Solución propuesta

- Extensión al protocolo de BitTorrent. Dos capas:
  - Identidad digital: autenticación y autorización.
  - Gestión de la reputación.
- Esquema confederado:
  - Cada *tracker* actúa como una federación local. Un *peer* “pertenece” a un tracker.
  - La federación de *trackers* permite la ubicuidad de los *peers*.

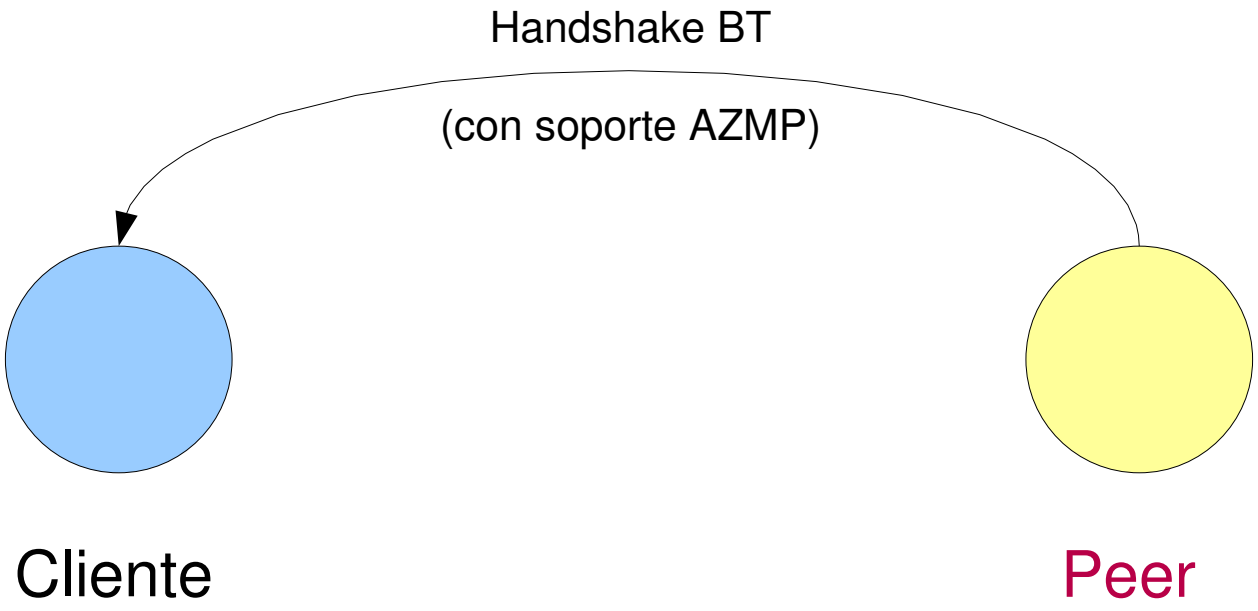
Solución propuesta

- Modelo de identidad digital
  - Basado en:
    - PKI, local o global.
    - eduGAIN, arquitectura AAI.
  - Conceptos básicos:
    - *Home tracker:* el *tracker* que **garantiza** la **identidad** de un *peer*, y **almacena** su **reputación**.
    - *Remote tracker:* el *tracker* al que se encuentra **conectado actualmente** un *peer*.
    - *Peer* o *par:* cualquier cliente BitTorrent.
    - *Usuario:* cliente BitTorrent del usuario.

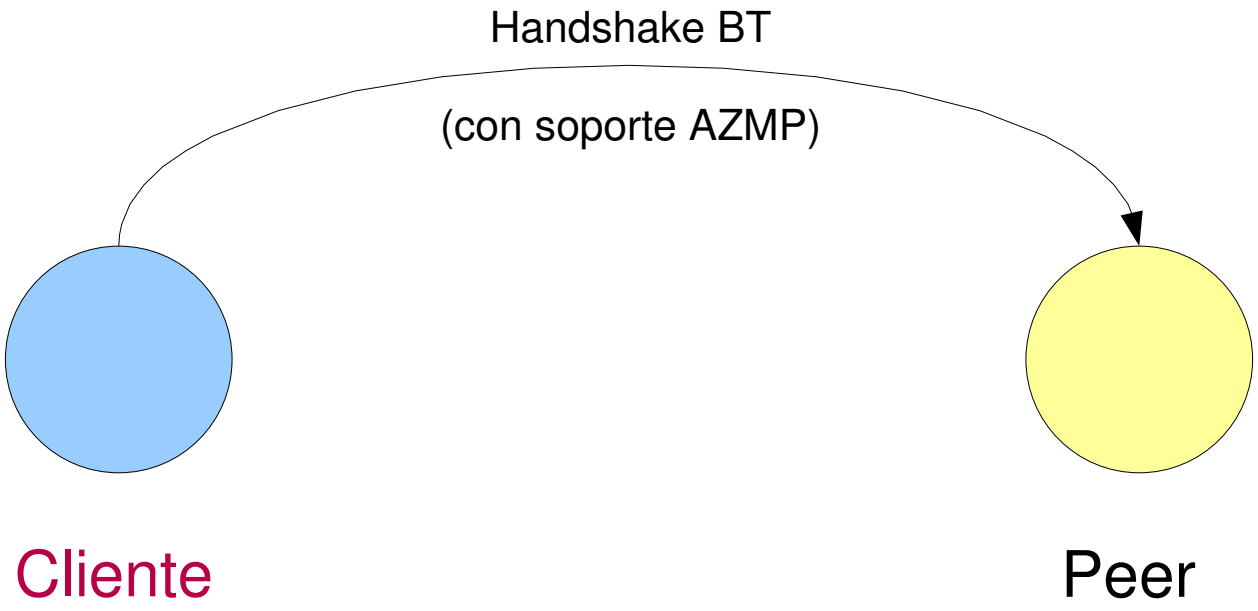
- Modelo de identidad basado en PKI



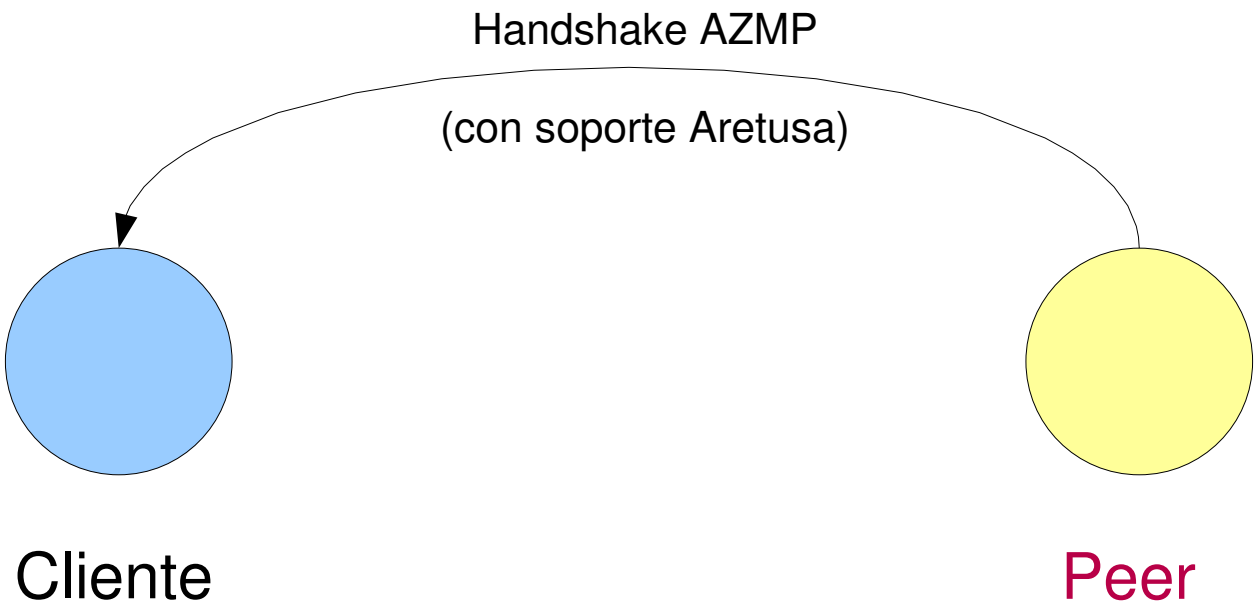
- Interacción entre pares



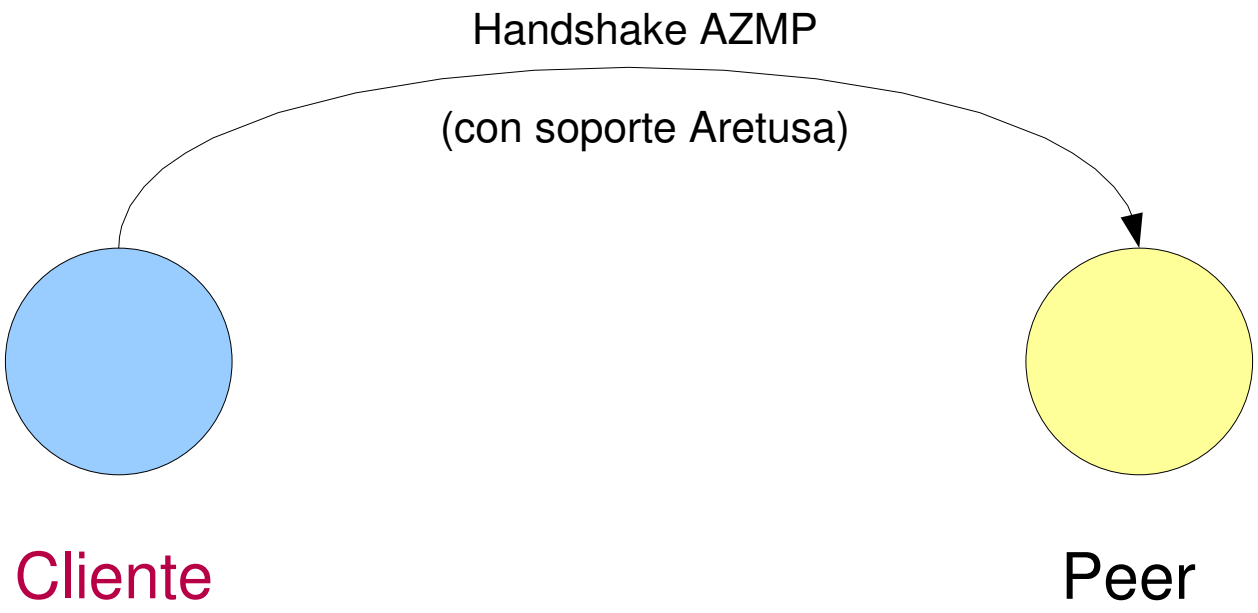
- Interacción entre pares



- Interacción entre pares

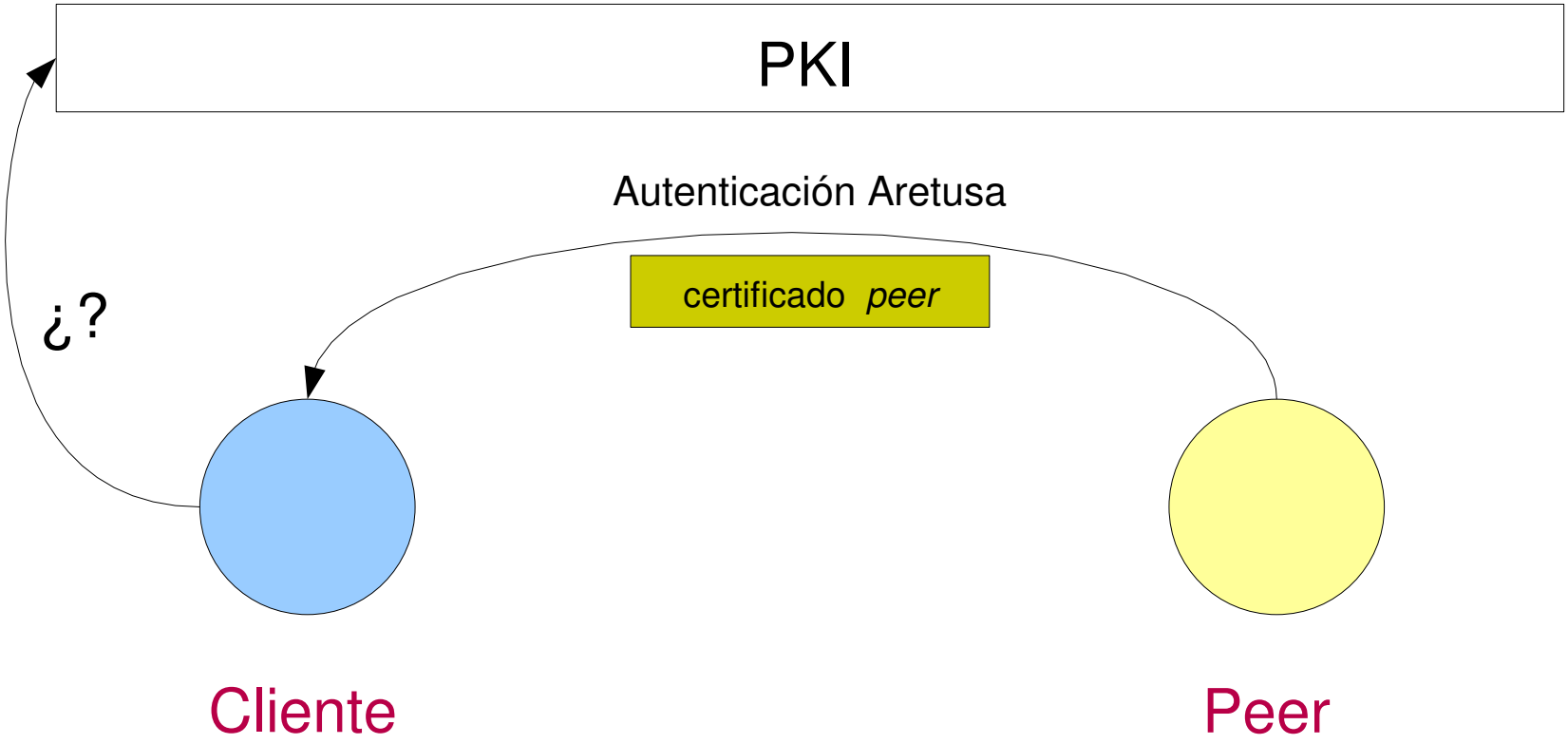


- Interacción entre pares

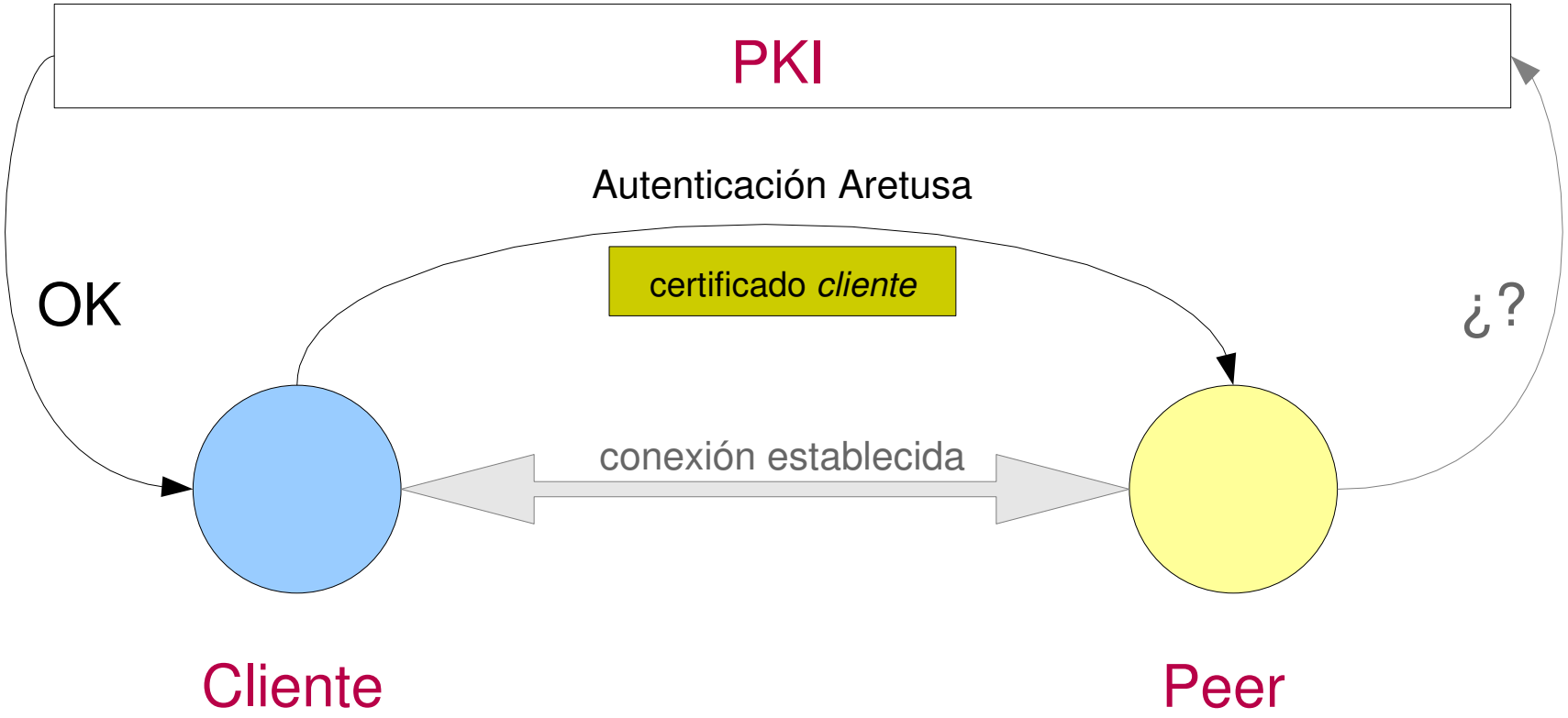


Solución propuesta

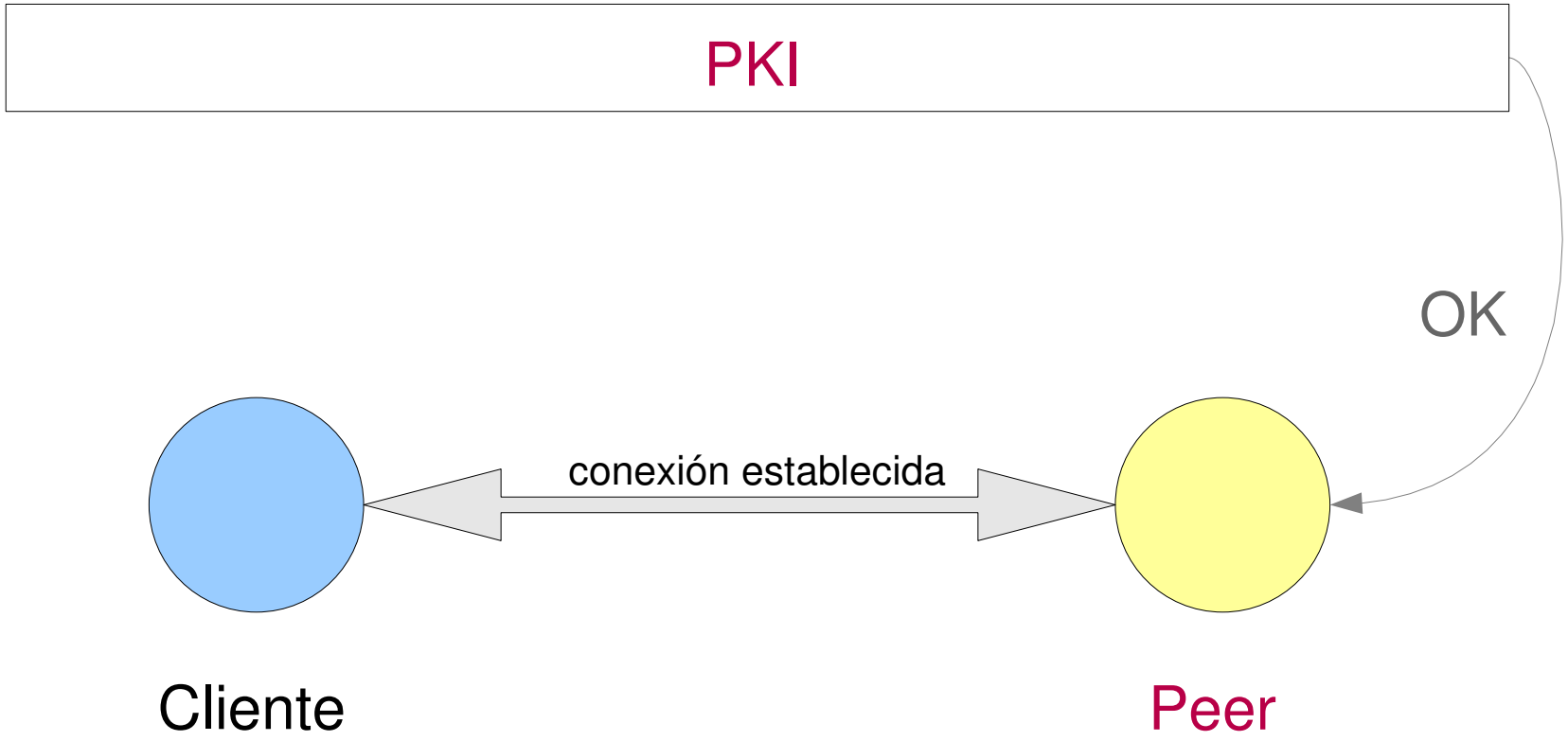
- Interacción entre pares



- Interacción entre pares



- Interacción entre pares



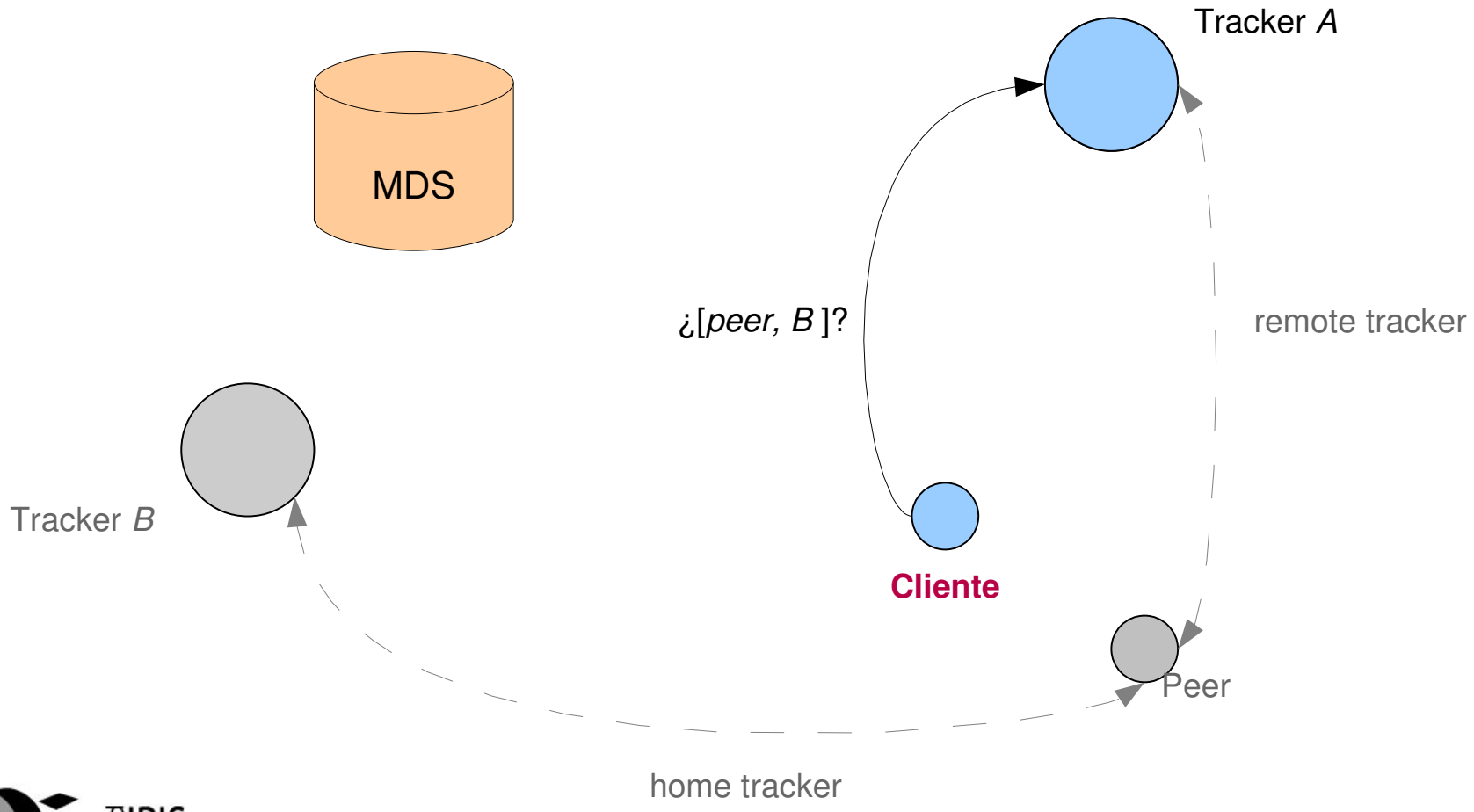
Solución propuesta

- ¿Qué ocurre si un par no es capaz de autenticar a otro por su certificado?
  - Se deja al criterio del implementador. Cada implementación puede decidir cómo actuar en este caso.
    - En redes con requisitos más relajados en las que sólo importa tener identificados al resto de pares, se puede **seguir adelante** con la conexión.
    - En redes en las que la identidad es básica (queremos estar seguros de que el par está certificado por alguien de nuestra confianza), se debe **cerrar la conexión**.

Solución propuesta

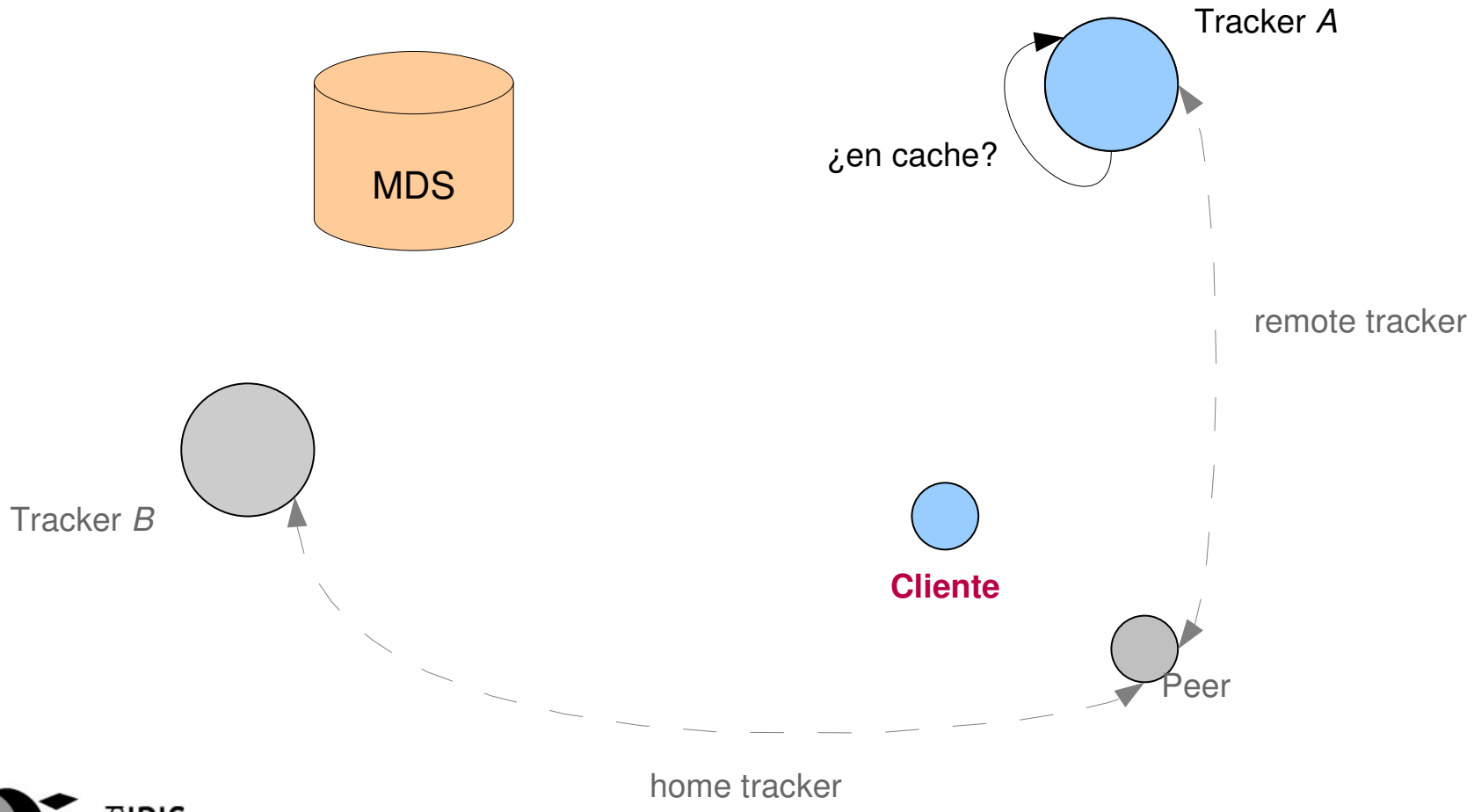
- Petición de reputación de un par
  - Primero es necesario comprobar quién certifica al par.
    - Si el *home tracker* del par es el *home tracker* del cliente, se consulta directamente a dicho *tracker*.
    - En caso contrario, el cliente pide al *MDS* información para localizar al *home tracker* del par y autenticarlo.

- Consulta al MDS (Servicio de Metadatos de eduGAIN)

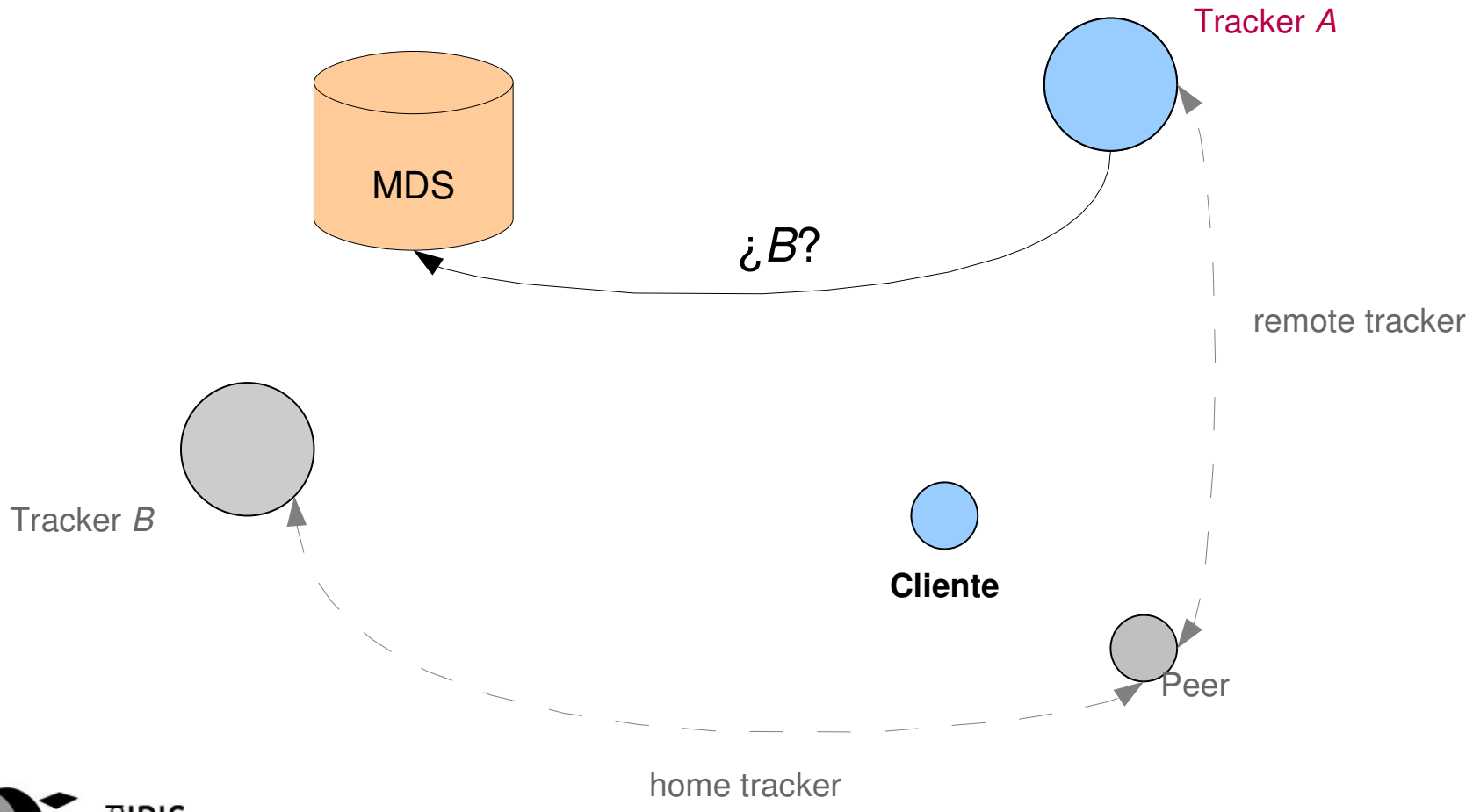


Solución propuesta

- Consulta al MDS (Servicio de Metadatos de eduGAIN)

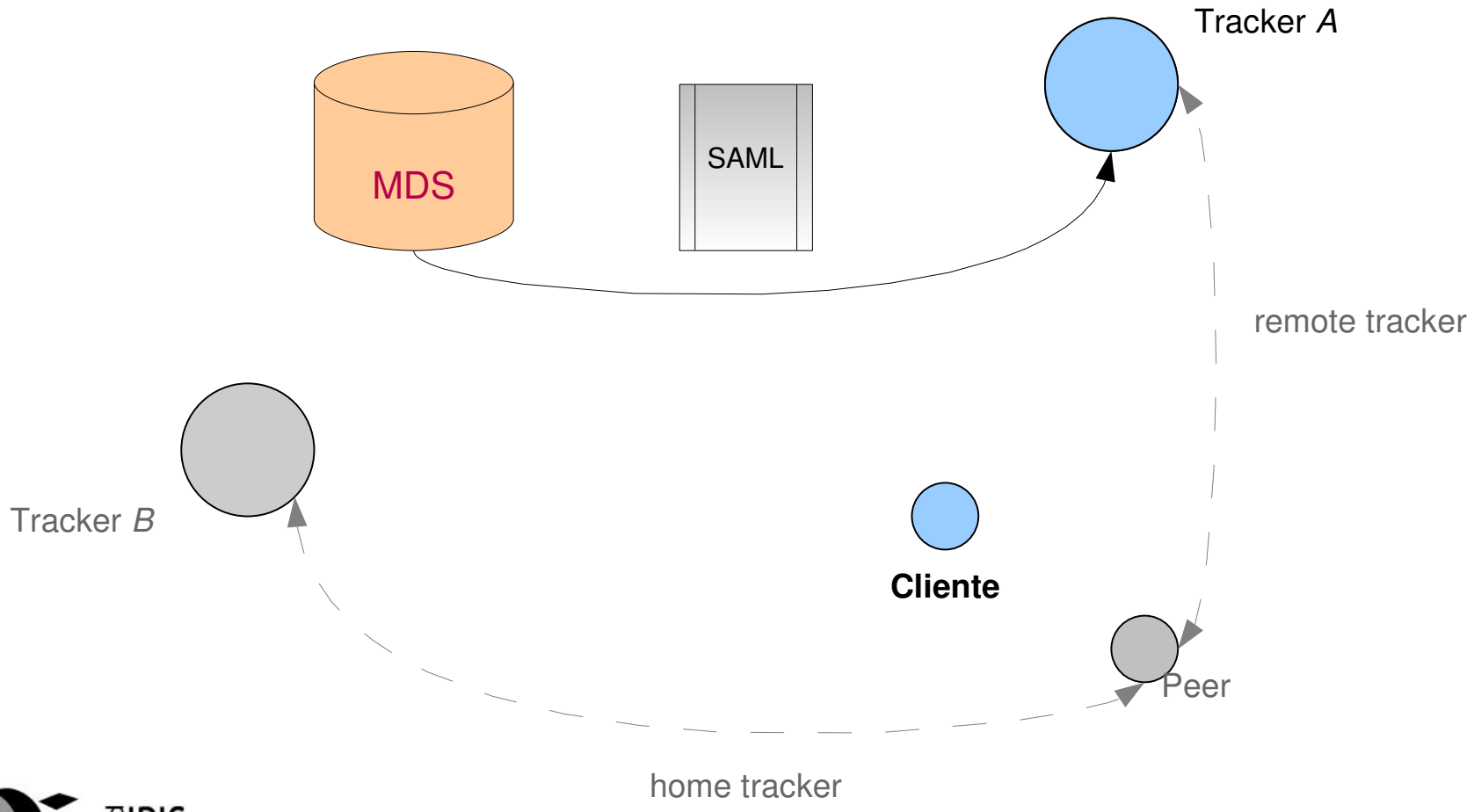


- Consulta al MDS (Servicio de Metadatos de eduGAIN)



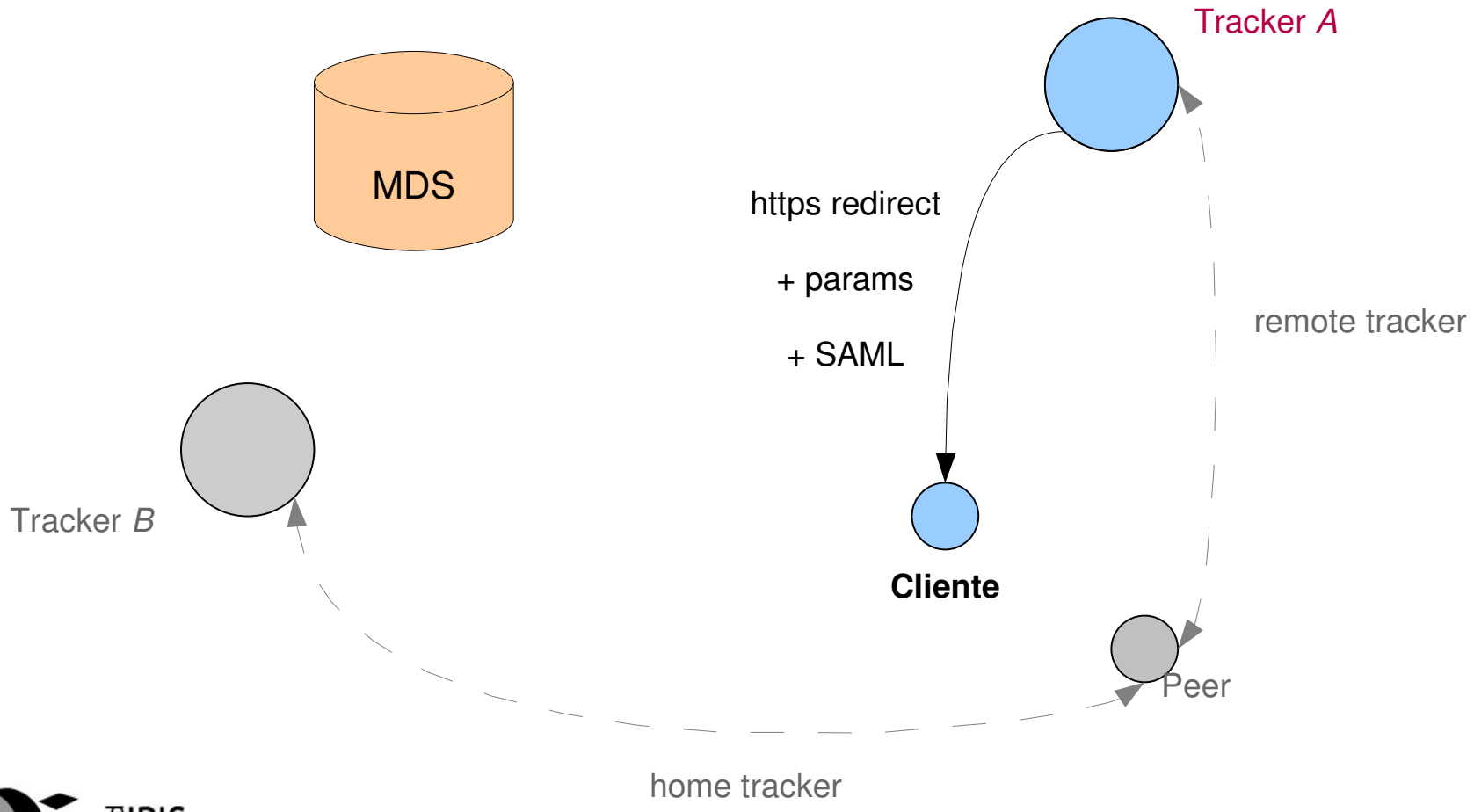
Solución propuesta

- Consulta al MDS (Servicio de Metadatos de eduGAIN)



Solución propuesta

- Consulta al MDS (Servicio de Metadatos de eduGAIN)



Solución propuesta

- Notificación de reputación de un par
  - Igual que la petición de reputación.
  - En lugar de pedir la URL de autenticación, se pide la de notificación.
  - Los *home_tracker* **deben** autenticar siempre a los pares que notifican reputación de uno de sus pares para evitar malos usos.
  - Cada notificación debería quedar registrada:
    1. Par que notifica.
    2. Par sobre el que se notifica.
    3. Reputación.

Solución propuesta

- Servicio de metadatos
  - Proporcionado por eduGAIN.
  - Almacena metadatos (documentos XML) sobre cada elemento en la red.
  - Siempre se deben verificar las conexiones con el MDS y validar las firmas que este emite por cada documento.

Implementación: Aretusa

- Actualmente: en desarrollo.
- Basado en Azureus (cliente BT).
- Utiliza *AZMP* (protocolo de extensión).
- En forma de plugins java.

Preguntas

red.es

Red IRIS

Edificio Bronce
Plaza Manuel Gómez Moreno s/n
28020 Madrid. España

Tel.: 91 212 76 20 / 25
Fax: 91 212 76 35
www.red.es