TACITES

Lot 3a2

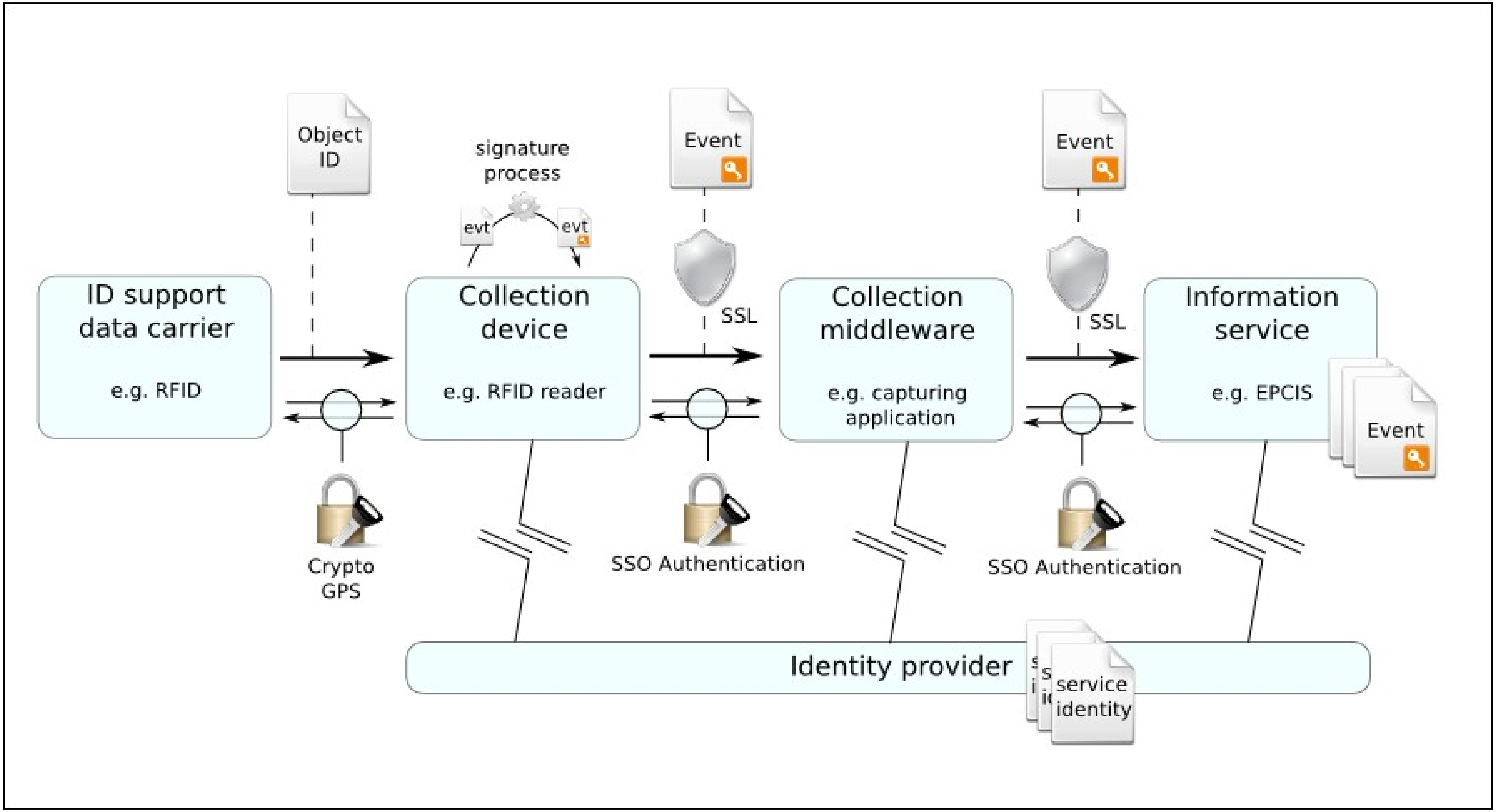
Network and Middleware Security

09/06/2011

Adrien Laurence : adrien.laurence@unicaen.fr

TACITES Lot 3a2 network and middleware Security

- General architecture -



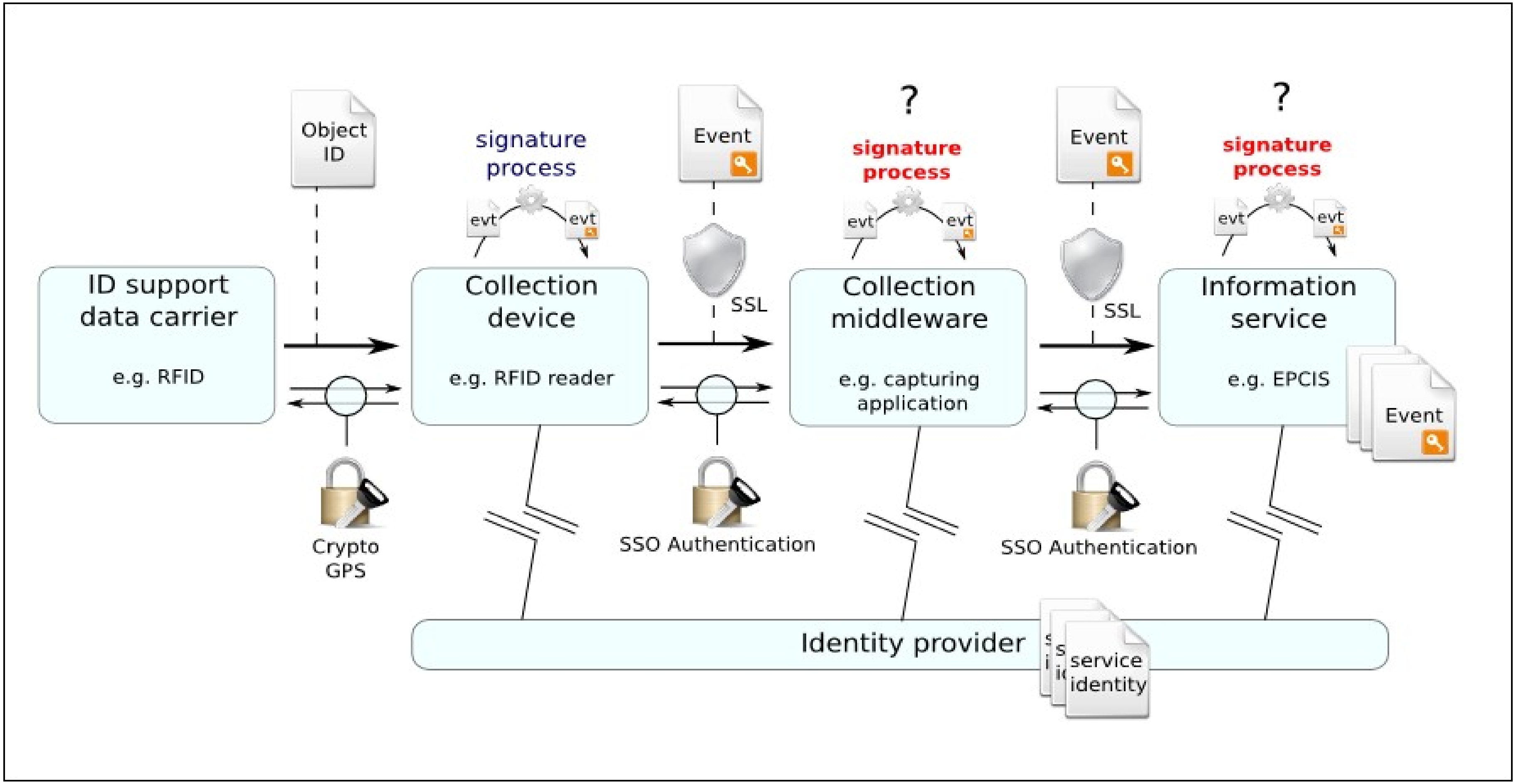
🔑 integrity

🛡 confidentiality

🔒 authentication

TACITES Lot 3a2 network and middleware Security

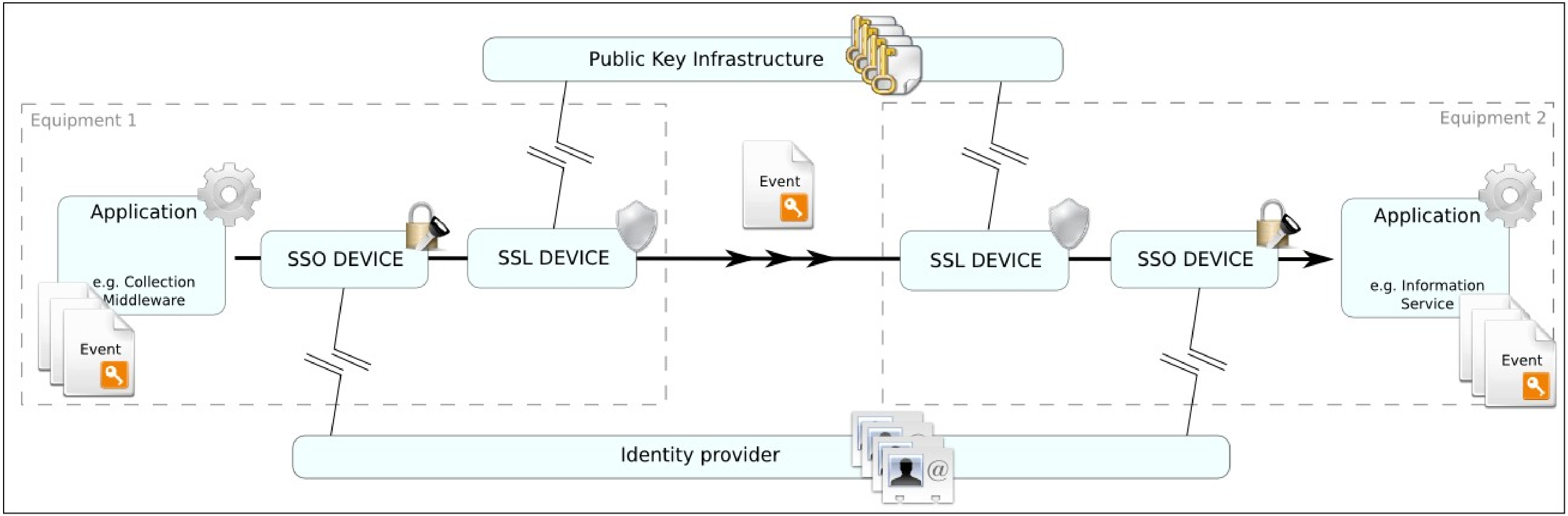
- general architecture – alternative -



- Digital signature in **each component** ?
  - *Sign message with or without previous signatures ?*
  - *Has to be inside events.*
    - How to store signatures in events ?
    - Signature can't be processed in external generic component (the signature component has to know about the format of the event)

TACITES Lot 3a2 network and middleware Security

- *Security components* -



SSO Device (Single Sign On Device) enables applications to mutually authenticate (CAS, Shibboleth, LASSO)

- Uses **identity provider**
- May be disconnected from identity provider.

SSL Device (Security Service Layer Device) enables applications to communicate through a secured Chanel (SSH, Apache2 SSL/TLS , VPN, IPSEC + DNSSEC)

- Provides bilateral authentication
- Uses PKI for encryption.
- May be disconnected from the PKI.

TACITES Lot 3a2 network and middleware Security

- Security component technologies -

SSO implémentations :

- **Shibboleth :**
  - Web single sign-on across or within organizational boundaries.
  - A standards based, open source software package.
  - Allows sites to make informed authorization decisions for individual access of protected online resources in A privacy-preserving manner.
  - Provides federation mechanisms.

- **CAS (Central Authentication Service) :**
  - "Single Sign-on for the Web"
  - Developed by JA-SIG in an open-source, collaborative manner.
  - Beneficial where applications share a set of common users.
  - Similar to the Shibboleth but :
    - vastly simpler to set up
    - lacks a number of broader features like federated trust and authorization infrastructure.

- **LASSO :**
  - A free software C library.
  - Implements the Liberty Alliance standards.
  - Defines processes for federated identities, single sign-on and related protocols.
  - Built on top of libxml2, XMLSec and OpenSSL.
  - Licensed under the GNU General Public License (with an OpenSSL exception).

TACITES Lot 3a2 network and middleware Security

- Security component technologies -

Secured transport layer technologies :

- **Stunnel / Openvpn :**
  - Virtual Private Network (VPN).
  - Secured tunneling applications.
  - Can be used to send any kind of network traffic securely.

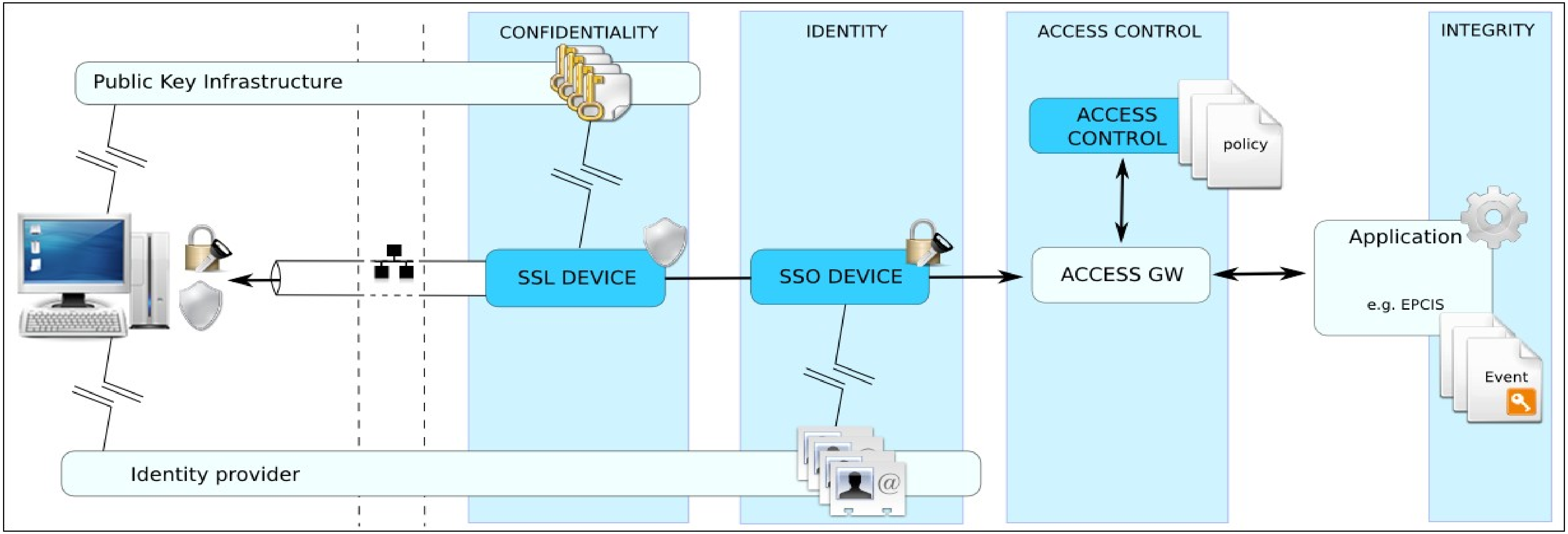
- **Apache2 SSL/TLS encryption :**
  - Provides strong cryptography for the Apache webserver.
  - Use Secure Sockets Layer (SSL v2/ v3) and Transport Layer Security (TLS v1) protocols.
  - Use Open Source SSL/TLS toolkit OpenSSL.
  - Only used to send HTTP(S) traffic.

- **IPSEC (Internet Protocol Security) + DNSSEC :**
  - Is a protocol suite for securing Internet Protocol (IP) communications.
  - Protects any application traffic across an IP network.
  - Applications do not need to be specifically designed to use IPsec.
  - It authenticate and encrypte each IP packet of a communication session.
  - Includes protocols for establishing mutual authentication between agents at the beginning of the session And negotiation of cryptographic keys to be used during the session.
  - Hard to set up in an open network with a large set of computers and servers.
  - Involve setting up DNSSEC (public keys are stored in the DNS).

- **SSH :**
  - Allows data to be exchanged using a secure channel between two networked devices.
  - Uses public-key cryptography to authenticate the remote computer.

TACITES Lot 3a2 network and middleware Security

- Security layer & access control -



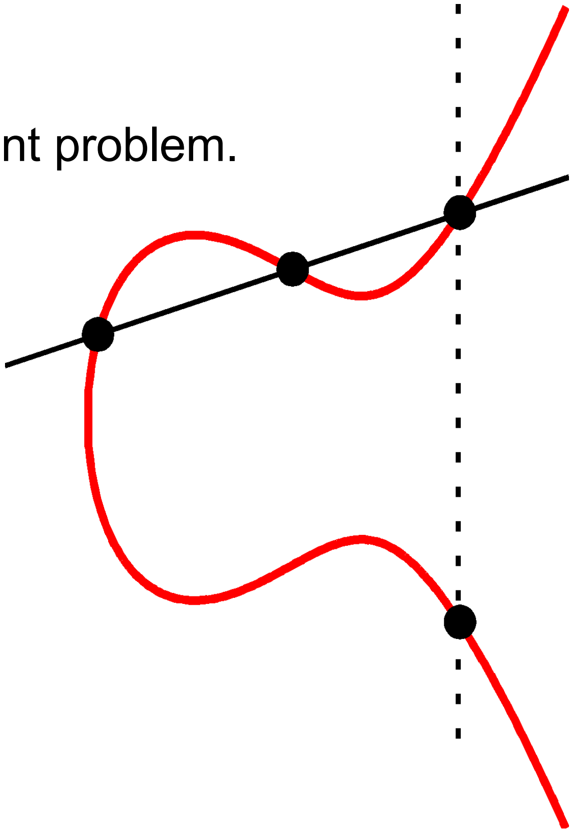
Access Control Layer : Enable service provider to restrict access to the data.

- Using access gateway (implementing application protocol) that forwards messages and filters responses. → *Non normative component*
- Accessible through normalized protocol (e.g XACML)

Integrity support : digital signature that enforces data integrity. (**GPS**,DSA,**EC-DSA**,RSA ...)

- Which technologie for signature ? -

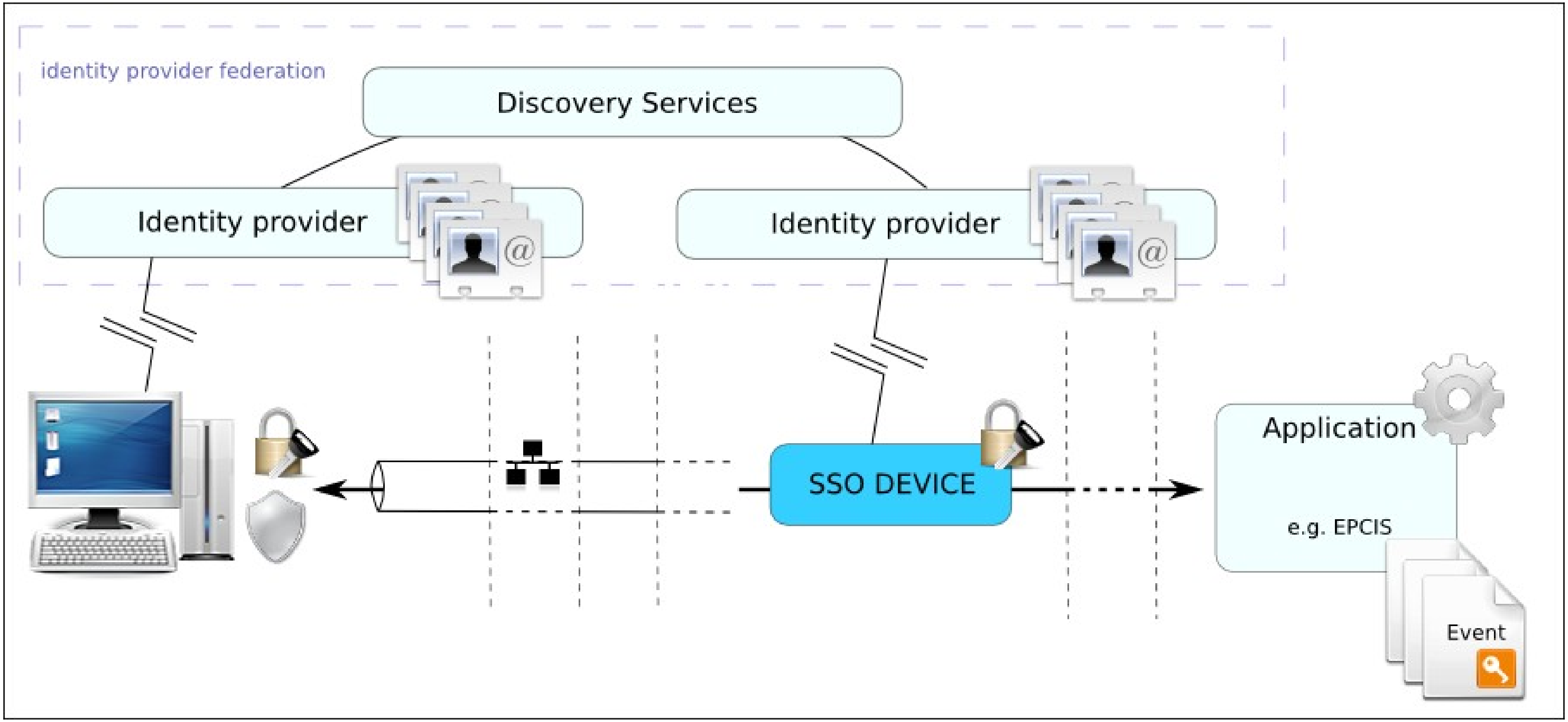
- GPS [Girault-Poupard-Stern JoC06]
  - Classical construction (authentication + Fiat-Shamir).
  - Fast signing process with fast modular arithmetic.
  - Support elliptic curves.
  - The security relies on the Discrete Log with Small Exponent problem.
  - Even faster with "coupons".
  - **1024 bits.**



- Alternatives :
  - standards : (EC)DSA (US), Esign (Japan).
  - RSA-PSS.
  - Short signatures (elliptic curves + pairing). **160 bits**
    - **Supports batch verifications**
  - Bernstein's signatures. **QUICKLY**

TACITES Lot 3a2 network and middleware Security

- Identity federation -



Identity Provider Federation : Connect several identity provider using discovery services mechanisms (e.g. Shibboleth).