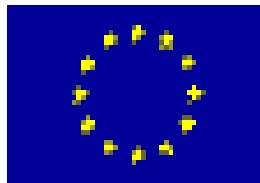




# Mobile Workers' Secure Business Applications in Ubiquitous Environments

Credentials and Policies  
Thijs Veugen (TNO)



[www.mosquito-online.org](http://www.mosquito-online.org)

# Contents

---

- Introduction to MOSQUITO
- Architecture for security decisions
- Security policies
- Credentials
- Infrastructure



# Background

---

- Specific Targeted Research Project (STREP) within the Sixth Framework Programme
  - STREP: 137 submitted / 31 ranked / 9 selected
    - MOSQUITO
- Strategic objective 2.3.2.6
  - Applications and Services for the Mobile User and Worker
- Finance
  - Overall: 267.3 PM / 3570.8 K€ cost / 1850.0 K€ grant
- Duration
  - 1 Sep 2004 – 31 Aug 2006



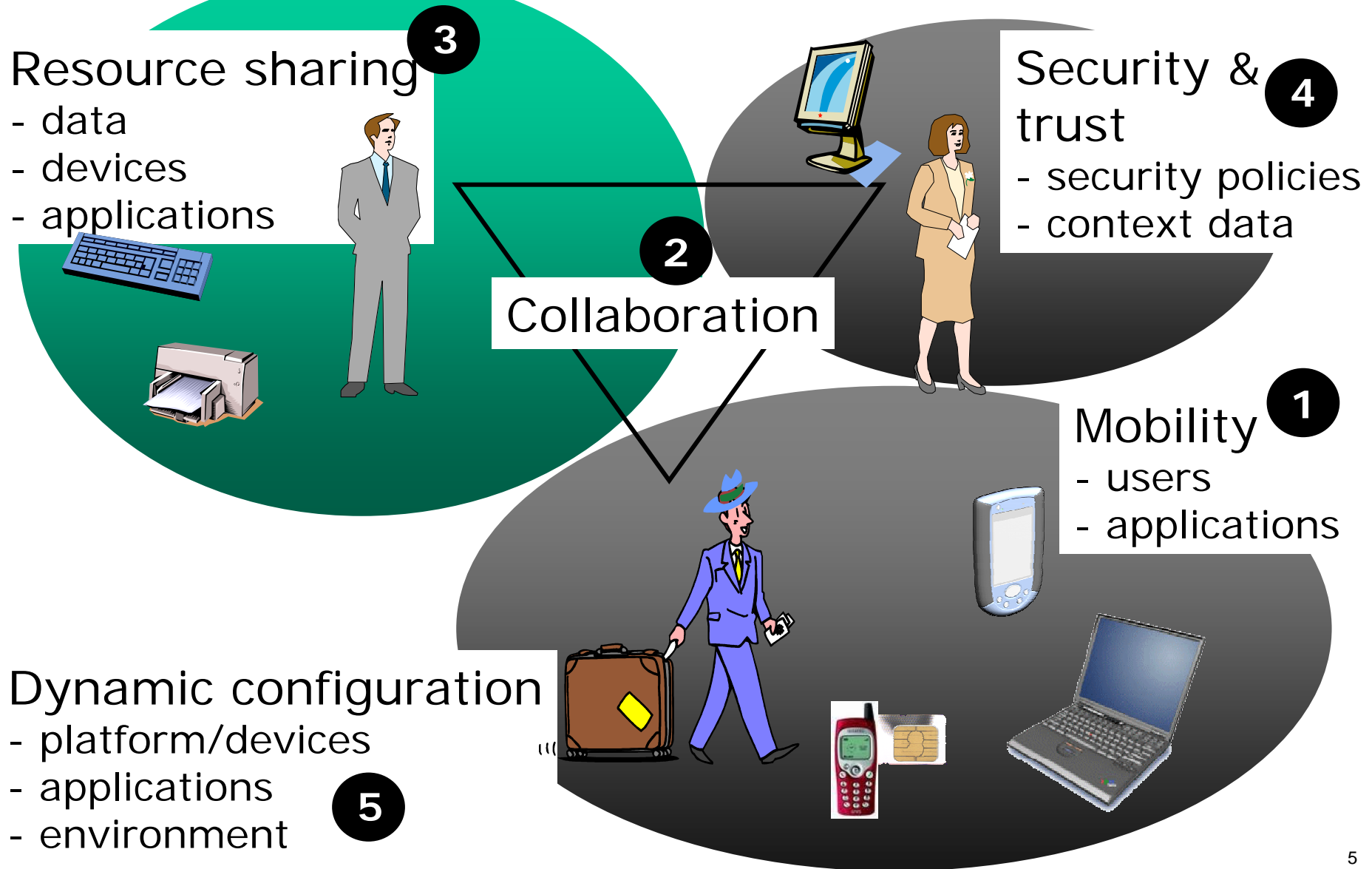
## MOSQUITO vision

---

- MOSQUITO ensures easy-to-use business applications security for mobile workers in **ubiquitous environments**:
  - Supporting the interactions of mobile workers with their clients across **multiple administrative domains** in a collaborative style
  - Allowing for **dynamic configurations** of mobile workers' devices across administrative domains
  - Using **mobile equipment** being adaptive to actual communication environments and processing capabilities
  - Make use of **security** mechanisms enforcing mobile workers' company's security policies



# Challenges

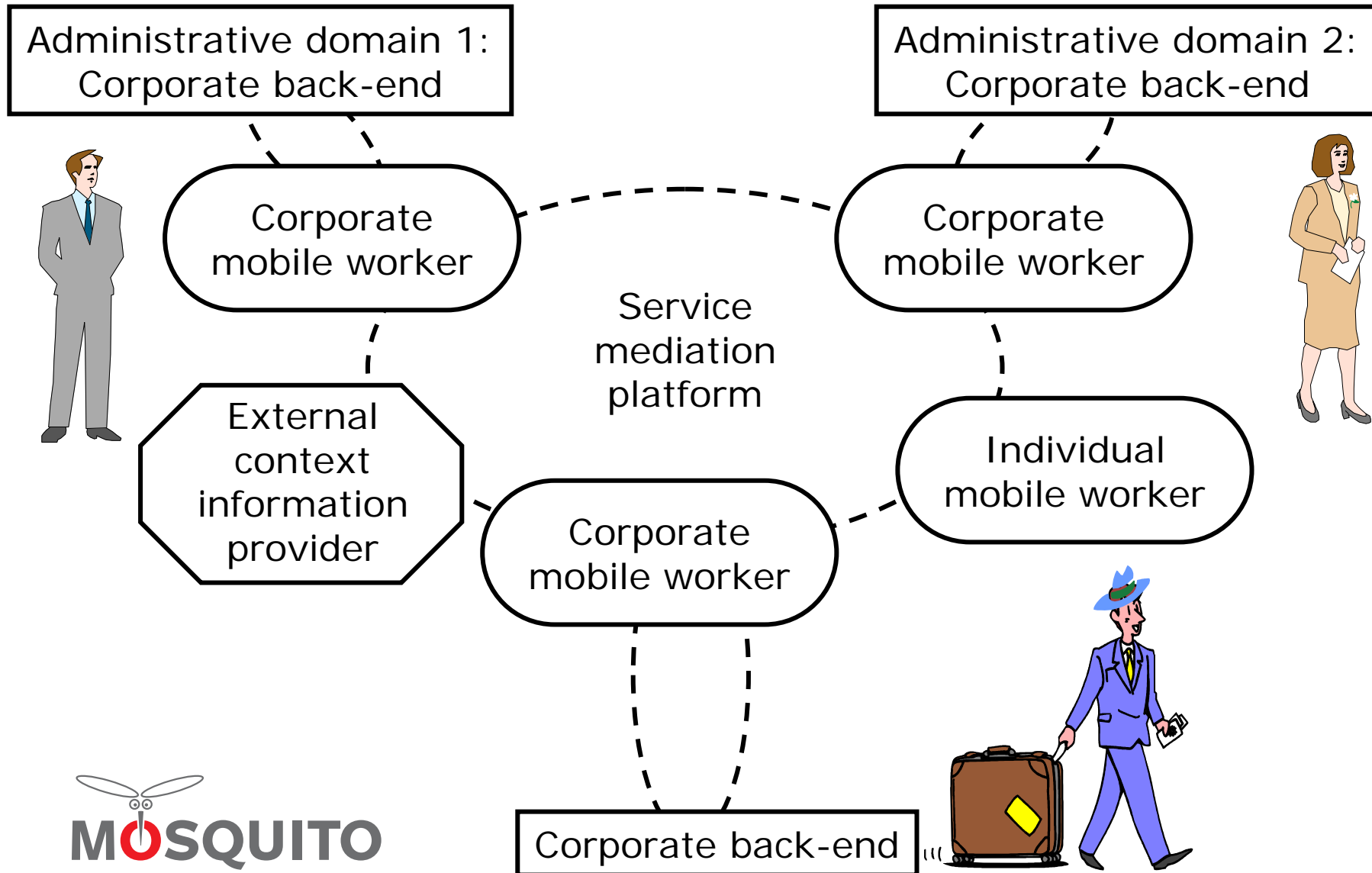


# Objectives

---

- To develop a **framework** for definition, management, and enforcement of security policies in multiple administrative domains;
- To design and develop context aware security and trust services; to implement a **trusted context information provider**;
- To specify and implement **service adaptation layer** to facilitate seamless integration of applications and services; especially dealing with context aware security and trust;
- To integrate **context awareness** in business applications as well as provide a common interface to interact with distributed mobile services in a collaborative fashion.

# Service mediation & context-awareness



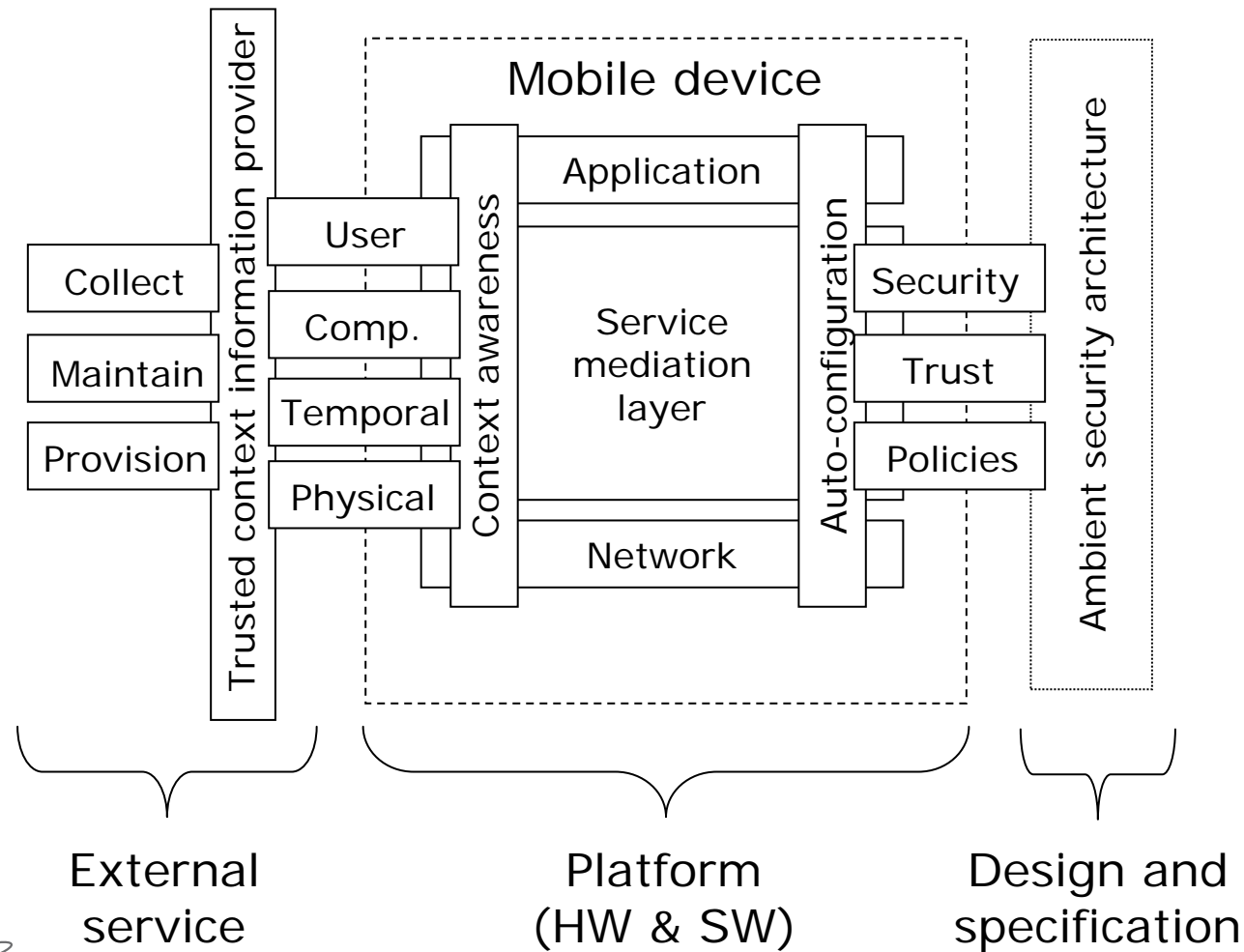
# Approach

---

- MOSQUITO will provide a **service mediation layer** with horizontal and vertical interface for collaboration of business applications in dynamic mobile environments
- The service mediation layer will flexibly **integrate device platforms based on mayor standards**
- It will provide the **integration of applications, context information, security, trust and policy services**
- Context information is retrieved from the **trusted context information service provider**
- Entities in the architecture will **access context information and trigger respective actions** subsequently; such as the auto-configuration of applications, services, and devices

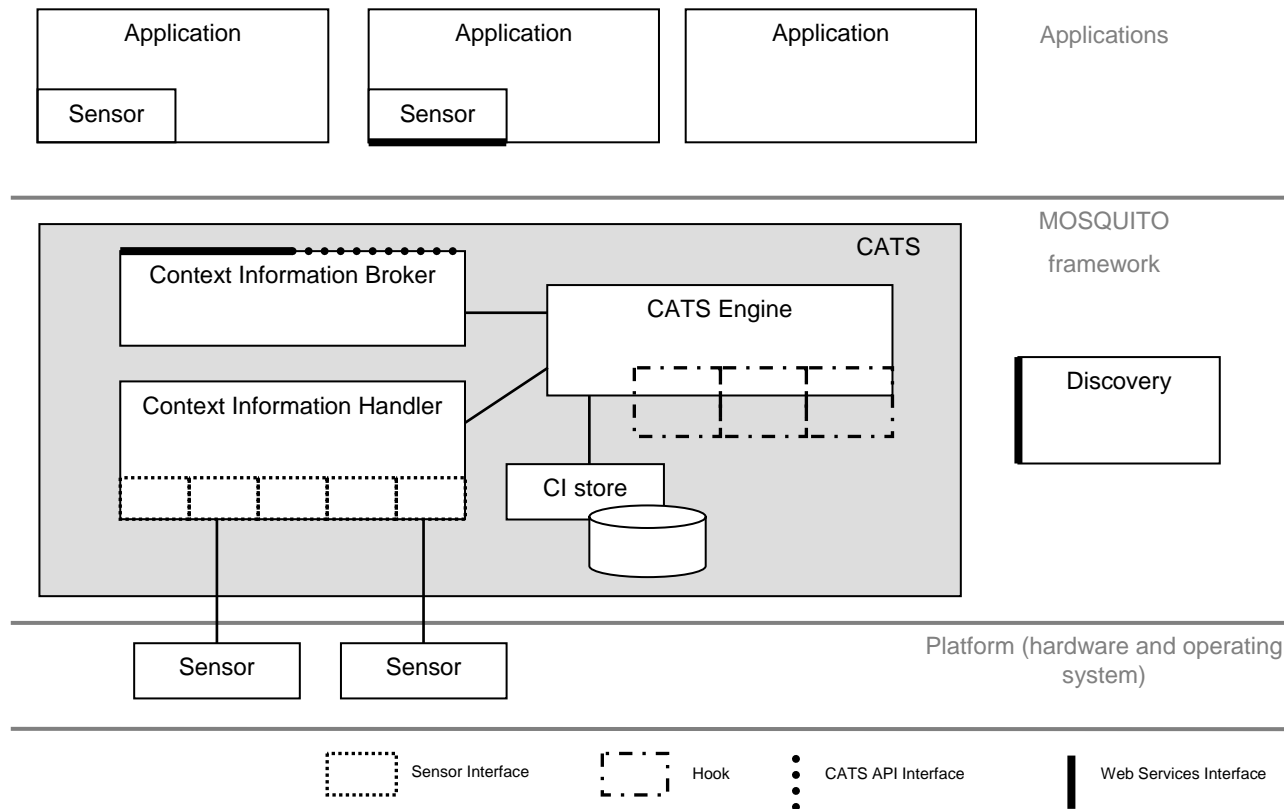


# Services integration





# CATS



## Security policies

---

- Low level policies to protect the integrity and confidentiality of MOSQUITO messages
- High level policies: defined by applications that use the MOSQUITO framework:
  - Trust (signatures, reputation)
  - Access Control
  - Federation: users exchanging data and/or programs by device-federation or delegation
  - Service discovery: client discovery and server publication
  - Privacy
  - Code verification (hooks)

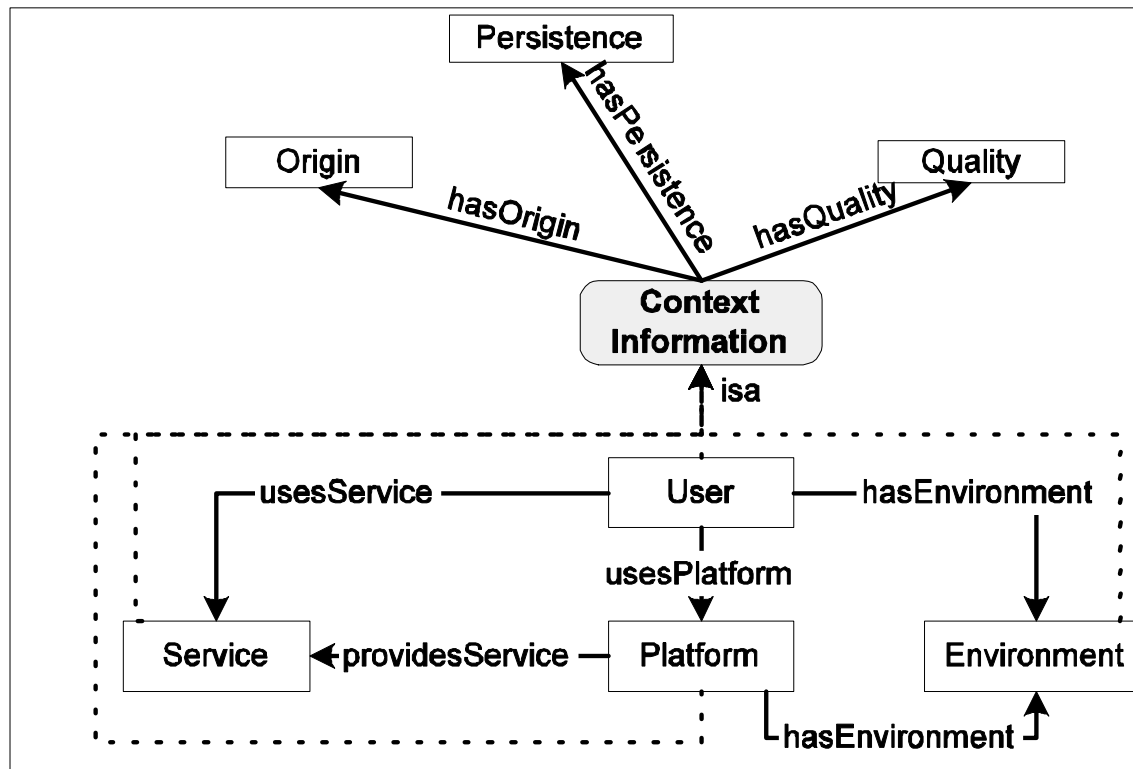


## Adding context awareness to policies

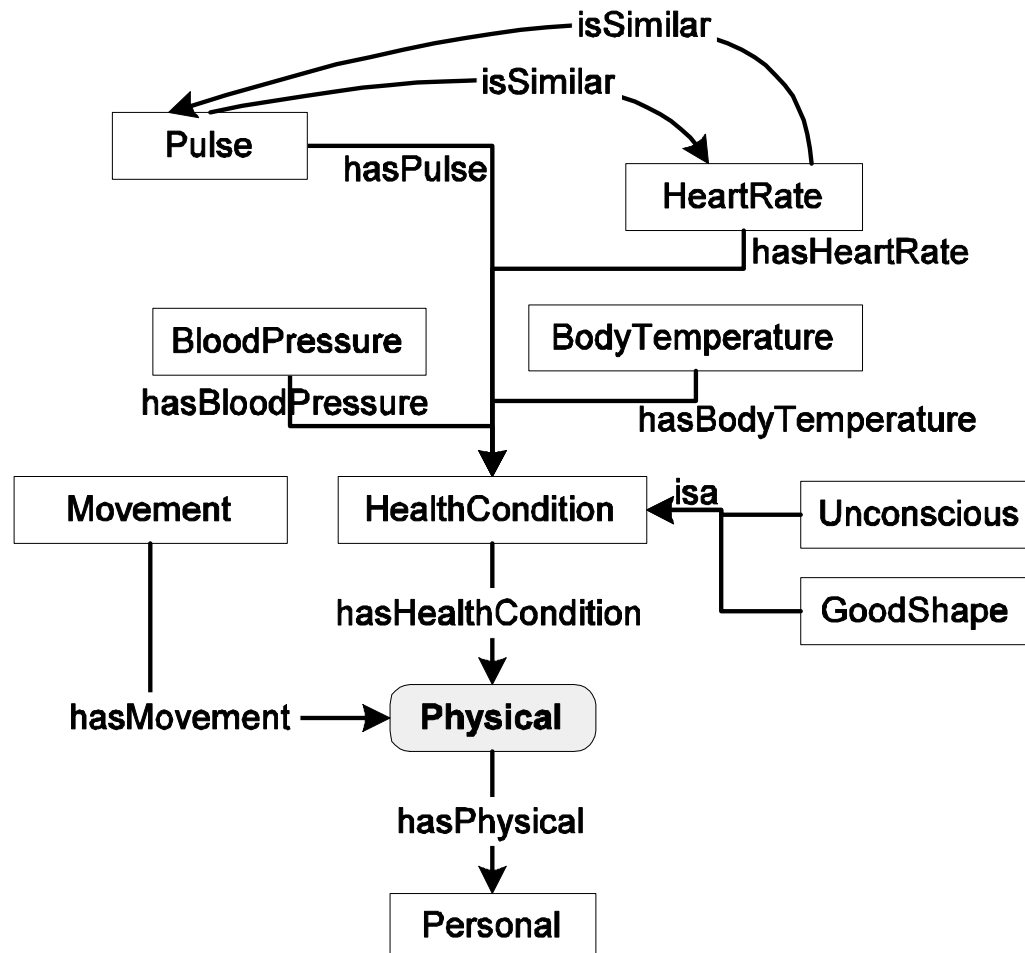
---

- Application oriented approach:  
ad-hoc XML vocabulary related to a specific application
- Model oriented approach:  
semi-formal conceptual models using UML
- Ontology oriented approach:  
knowledge representation and reasoning based on ontologies (OWL)

# Context Information in CoOL



# Reasoning



# OWL reasoning example

---

isUnconscious := User has Pulse below 50 and Blood Pressure below 50

- `<xsd:simpleType name="below10">`
  - `<xsd:restriction base="xsd:positiveInteger">`
  - `<xsd:maxInclusive value="50">`
  - `</xsd:restriction>`
- `</xsd:simpleType>`
- `<owl:Class rdf:ID="isUnconscious">`
  - `<owl:intersectionOf rdf:parseType="Collection">`
    - `<owl:Class rdf:about="#User"/>`
      - `<owl:Restriction>`
        - `<owl:onProperty rdf:resource="#Pulse">`
        - `<owl:someValuesFrom rdf:resource="#below10">`
      - `</owl:Restriction>`
  - `</owl:intersectionOf>`
  - `<owl:intersectionOf rdf:parseType="Collection">`
    - `<owl:Class rdf:about="#User"/>`
      - `<owl:Restriction>`
        - `<owl:onProperty rdf:resource="#BloodPressure">`
        - `<owl:someValuesFrom rdf:resource="#below10">`
      - `</owl:Restriction>`
  - `</owl:intersectionOf>`
- `</owl:Class>`



# OWL reasoning example

isUnconscious := User has Pulse below 50 and Blood Pressure below 50

- `<xsd:simpleType name="below10">`
  - `<xsd:restriction base="xsd:positiveInteger">`
  - `<xsd:maxInclusive value="50">`
  - `</xsd:restriction>`
- `</xsd:simpleType>`
- `<owl:Class rdf:ID="isUnconscious">`
  - `<owl:intersectionOf rdf:parseType="Collection">`
    - `<owl:Class rdf:about="#User"/>`
    - `<owl:Restriction>`
      - `<owl:onProperty rdf:resource="#Pulse">`
      - `<owl:someValuesFrom rdf:resource="#below10">`
    - `</owl:Restriction>`
  - `</owl:intersectionOf>`
  - `<owl:intersectionOf rdf:parseType="Collection">`
    - `<owl:Class rdf:about="#User"/>`
    - `<owl:Restriction>`
      - `<owl:onProperty rdf:resource="#BloodPressure">`
      - `<owl:someValuesFrom rdf:resource="#below10">`
    - `</owl:Restriction>`
  - `</owl:intersectionOf>`
- `</owl:Class>`



# OWL reasoning example

isUnconscious := User has Pulse below 50 and Blood Pressure below 50

- `<xsd:simpleType name="below10">`
  - `<xsd:restriction base="xsd:positiveInteger">`
  - `<xsd:maxInclusive value="50">`
  - `</xsd:restriction>`
- `</xsd:simpleType>`
- `<owl:Class rdf:ID="isUnconscious">`
  - `<owl:intersectionOf rdf:parseType="Collection">`
    - `<owl:Class rdf:about="#User"/>`
      - `<owl:Restriction>`
        - `<owl:onProperty rdf:resource="#Pulse">`
        - `<owl:someValuesFrom rdf:resource="#below10">`
      - `</owl:Restriction>`
  - `</owl:intersectionOf>`
  - `<owl:intersectionOf rdf:parseType="Collection">`
    - `<owl:Class rdf:about="#User"/>`
      - `<owl:Restriction>`
        - `<owl:onProperty rdf:resource="#BloodPressure">`
        - `<owl:someValuesFrom rdf:resource="#below10">`
      - `</owl:Restriction>`
  - `</owl:intersectionOf>`
- `</owl:Class>`



# OWL reasoning example

isUnconscious := User has Pulse below 50 and Blood Pressure below 50

- `<xsd:simpleType name="below10">`
  - `<xsd:restriction base="xsd:positiveInteger">`
  - `<xsd:maxInclusive value="50">`
  - `</xsd:restriction>`
- `</xsd:simpleType>`
- `<owl:Class rdf:ID="isUnconscious">`
  - `<owl:intersectionOf rdf:parseType="Collection">`
    - `<owl:Class rdf:about="#User"/>`
      - `<owl:Restriction>`
        - `<owl:onProperty rdf:resource="#Pulse">`
        - `<owl:someValuesFrom rdf:resource="#below10">`
      - `</owl:Restriction>`
  - `</owl:intersectionOf>`
  - `<owl:intersectionOf rdf:parseType="Collection">`
    - `<owl:Class rdf:about="#User"/>`
      - `<owl:Restriction>`
        - `<owl:onProperty rdf:resource="#BloodPressure">`
        - `<owl:someValuesFrom rdf:resource="#below10">`
      - `</owl:Restriction>`
  - `</owl:intersectionOf>`
- `</owl:Class>`



# Policy languages used in MOSQUITO

---

## Security policy languages:

- XACML for access control:
  - Compatible with web services
  - SAML assertions to exploit context information
- REI for other purposes:
  - Ontology based
  - Usage of existing ontologies (e.g. context information)
  - Semantics enable reasoning and aggregation

## REI principals

---

- Actions: Action(Subject, Target, PreCondition, Effect)
- Speech acts:
  - Delegation (possibly revoked)
  - Request for (1) an action, or (2) a right
  - Revocation of (1) a received right, or (2) a delegation
  - Cancel (of a request)
- Deontic concepts of permissions, prohibitions (negative permissions), obligations and dispensations (waiver for obligations)
- Meta-policies for conflict resolution: override

# REI example

---

```
/--Access to a personal medical data --/
```

```
/-- To access medical data the requester Y must give a credential to proof  
that he is the personal physician of patient X--/
```

```
Obligation (Y, Query(X, Y, Access(Y, resources (X.medicalData.all()), Read)),  
Has (Y, Credential(physician()))AND Has (X, X.medicalData.Physician()==  
Y));
```

```
/-- To access medical data the requester Y must give a credential to proof  
that he has the permission to access data of patient X --/
```

```
Obligation (Y, Query(X, Y, Access(Y, resources (X.medicalData.all()), Read)),  
Has (Y, Right (Read, Credential(Y.medicalData.Access(Read))));
```

```
/-- To access medical data the requester Y must give a credential to proof  
that he has a role of physician or he is an emergency physician, that the  
patient X is in emergency case and the requester is near to the patient --/
```

```
Obligation (Y, query(X, Y, Access(Y, resources (X.medicalData.all()), Read),  
Condition (Context (closeTo(X.location()) AND state(X.emergencyCase()) AND  
Has (Y, Credential (Y.physician.emergency()) OR Has (Y, Role  
(physician()))));
```

# Credentials

---

- Credential := any data that is presented to establish a property of an entity (RFC 2828)
- The *issuer* certifies the contents of the credential (by using a digital signature)

# Credentials

---

- Credential := any data that is presented to establish a property of **an entity** (RFC 2828)
- The *issuer* certifies the contents of the credential (by using a digital signature)
- The *holder*

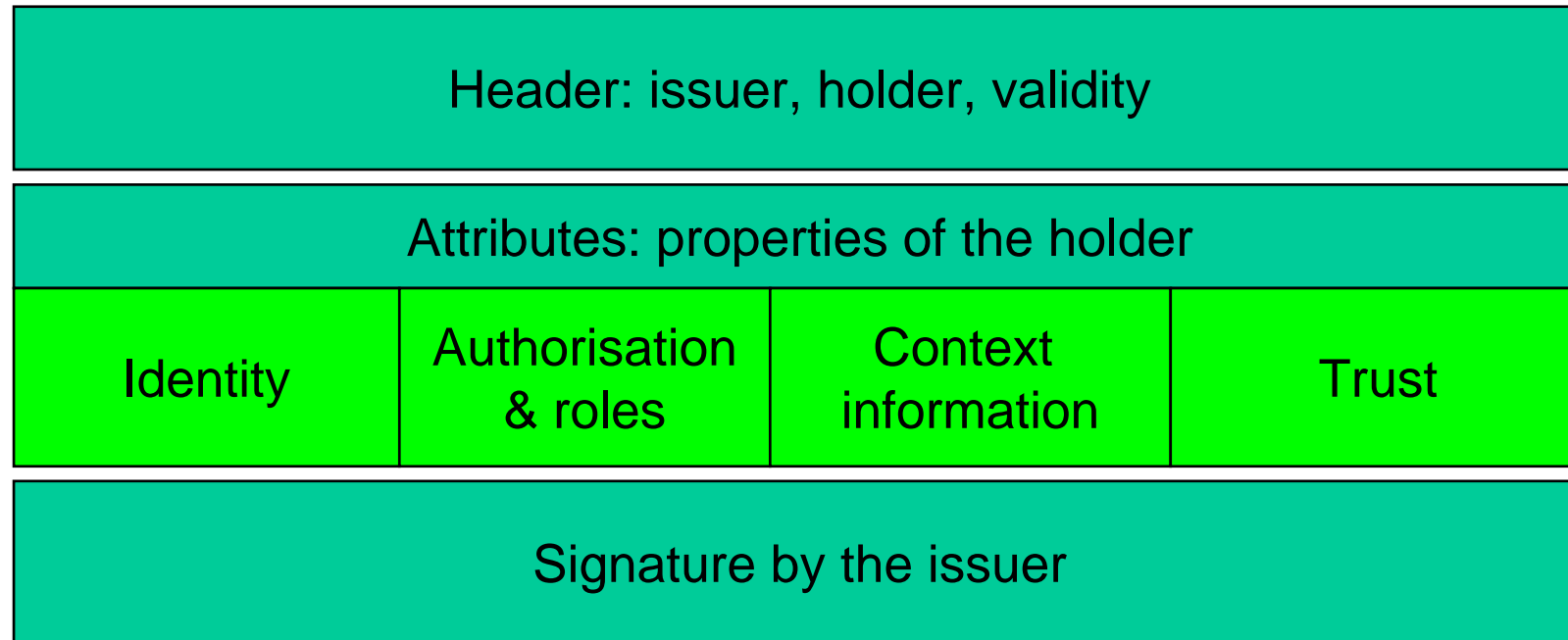
# Credentials

---

- Credential := any data that is presented to establish a **property** of an entity (RFC 2828)
- The *issuer* certifies the contents of the credential (by using a digital signature)
- Properties of the *holder*:
  - Identity: name, photo, authentication method
  - Role (in a group)
  - Authorisation: permissions
  - Trust: recommendation, certification, reputation
  - Context: location, presence, state

# Credentials

---



The credential is specified in XML using namespaces like W3C XML digital signature.

The MOSQUITO credential is compatible with SAML and EuréCA certificates



# Credential specification

---

```

<Credential:MosquitoCredential wsu:Id="SecurityCredential-ABC..."
  xmlns:Credential=http://mosquito-online.org/security/Credential
  xmlns:wss=http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd
  xmlns="http://www.w3.org/2000/09/xmldsig#">
  <Credential:Header>
    <Credential:CreatedAt>2005-06-21T06:50:50Z</Credential:CreatedAt>
    <Credential:ExpiresAt>2005-06-21T14:50:50Z</Credential:ExpiresAt>
    <Credential:Issuer>Issuer XY</Credential:Issuer>
    <Credential:Holder>Holder YZ</Credential:Holder>
  </Credential:Header>
  <Credential:Attributes>
    <Credential:IdAttribute>.....</Credential:IdAttribute>
    <Credential:AuthorisationAndRolesAttribute>.....</Credential:AuthorisationAndRolesAttribute>
    <Credential:ContextInformationAttribute>.....</Credential:ContextInformationAttribute>
    <Credential:TrustAttribute>.....</Credential:TrustAttribute>
  </Credential:Attributes>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
        xmlns:ds="http://www.w3.org/2000/09/xmldsig#" />
      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
      <Reference URI="#SecurityCredential-ABC...">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
          <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
        <DigestValue>VSkhxcLbHxyKf/0112014oWXUM=</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>e+W7AyNmVfL6Zp8N0RJMnUr16rW+0zYT3Ae/j2d3DA7v9j.../Q3E0sTNMWC9SJj7tLIp1JbLVomR74FKU=</SignatureValue>
  <KeyInfo>
    <wss:SecurityCredentialReference>
      <wss:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-tok...WuQ=</wss:KeyIdentifier>
    </wss:SecurityCredentialReference>
  </KeyInfo>
</Signature>
</Credential:MosquitoCredential>

```



# Credential specification – XML name spaces

```

<Credential:MosquitoCredential wsu:Id="SecurityCredential-ABC..."
  xmlns:Credential=http://mosquito-online.org/security/Credential
  xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd"
  xmlns="http://www.w3.org/2000/09/xmldsig#">
  <Credential:Header>
    <Credential:CreatedAt>2005-06-21T06:50:50Z</Credential:CreatedAt>
    <Credential:ExpiresAt>2005-06-21T14:50:50Z</Credential:ExpiresAt>
    <Credential:Issuer>Issuer XY</Credential:Issuer>
    <Credential:Holder>Holder YZ</Credential:Holder>
  </Credential:Header>
  <Credential:Attributes>
    <Credential:IdAttribute>.....</Credential:IdAttribute>
    <Credential:AuthorisationAndRolesAttribute>.....</Credential:AuthorisationAndRolesAttribute>
    <Credential:ContextInformationAttribute>.....</Credential:ContextInformationAttribute>
    <Credential:TrustAttribute>.....</Credential:TrustAttribute>
  </Credential:Attributes>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
        xmlns:ds="http://www.w3.org/2000/09/xmldsig#" />
      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
      <Reference URI="#SecurityCredential-ABC...">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
          <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
        <DigestValue>VSkhxcLbHxyKf/0112014oWXUM=</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>e+W7AyNmVfL6Zp8N0RJMnUr16rW+0zYT3Ae/j2d3DA7v9j.../Q3E0sTNMWC9SJz7tLIp1JbLVomR74FKU=</SignatureValue>
  <KeyInfo>
    <wsse:SecurityCredentialReference>
      <wsse:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-tok...WuQ=</wsse:KeyIdentifier>
    </wsse:SecurityCredentialReference>
  </KeyInfo>
</Signature>
</Credential:MosquitoCredential>

```



# Credential specification - Header

```

<Credential:MosquitoCredential wsu:Id="SecurityCredential-ABC..."
  xmlns:Credential=http://mosquito-online.org/security/Credential
  xmlns:wss=http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd
  xmlns="http://www.w3.org/2000/09/xmldsig#">
  <Credential:Header>
    <Credential:CreatedAt>2005-06-21T06:50:50Z</Credential:CreatedAt>
    <Credential:ExpiresAt>2005-06-21T14:50:50Z</Credential:ExpiresAt>
    <Credential:Issuer>Issuer XY</Credential:Issuer>
    <Credential:Holder>Holder YZ</Credential:Holder>
  </Credential:Header>
  <Credential:Attributes>
    <Credential:IdAttribute>.....</Credential:IdAttribute>
    <Credential:AuthorisationAndRolesAttribute>.....</Credential:AuthorisationAndRolesAttribute>
    <Credential:ContextInformationAttribute>.....</Credential:ContextInformationAttribute>
    <Credential:TrustAttribute>.....</Credential:TrustAttribute>
  </Credential:Attributes>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
        xmlns:ds="http://www.w3.org/2000/09/xmldsig#" />
      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
      <Reference URI="#SecurityCredential-ABC...">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
          <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
        <DigestValue>VSkhxcLbHxyKf/0112014oWXUM=</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>e+W7AyNmVfL6Zp8N0RJMnUr16rW+0zYT3Ae/j2d3DA7v9j.../Q3E0sTNMWC9SJj7tLIp1JbLVomR74FKU=</SignatureValue>
    <KeyInfo>
      <wss:SecurityCredentialReference>
        <wss:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-tok...WuQ=</wss:KeyIdentifier>
      </wss:SecurityCredentialReference>
    </KeyInfo>
  </Signature>
</Credential:MosquitoCredential>

```



# Credential specification - Attributes

```

<Credential:MosquitoCredential wsu:Id="SecurityCredential-ABC..."
  xmlns:Credential=http://mosquito-online.org/security/Credential
  xmlns:wss=http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd
  xmlns="http://www.w3.org/2000/09/xmldsig#">
  <Credential:Header>
    <Credential:CreatedAt>2005-06-21T06:50:50Z</Credential:CreatedAt>
    <Credential:ExpiresAt>2005-06-21T14:50:50Z</Credential:ExpiresAt>
    <Credential:Issuer>Issuer XY</Credential:Issuer>
    <Credential:Holder>Holder YZ</Credential:Holder>
  </Credential:Header>
  <Credential:Attributes>
    <Credential:IdAttribute>.....</Credential:IdAttribute>
    <Credential:AuthorisationAndRolesAttribute>.....</Credential:AuthorisationAndRolesAttribute>
    <Credential:ContextInformationAttribute>.....</Credential:ContextInformationAttribute>
    <Credential:TrustAttribute>.....</Credential:TrustAttribute>
  </Credential:Attributes>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
        xmlns:ds="http://www.w3.org/2000/09/xmldsig#" />
      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
      <Reference URI="#SecurityCredential-ABC...">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
          <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
        <DigestValue>VSkhxcLbHxyKf/0112014oWXUM=</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>e+W7AyNmVfL6Zp8N0RJMnUr16rW+0zYT3Ae/j2d3DA7v9j.../Q3E0sTNMWC9SJz7tLIp1JbLVomR74FKU=</SignatureValue>
  <KeyInfo>
    <wss:SecurityCredentialReference>
      <wss:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-tok...WuQ=</wss:KeyIdentifier>
    </wss:SecurityCredentialReference>
  </KeyInfo>
</Signature>
</Credential:MosquitoCredential>

```



# Credential specification - Signature

```

<Credential:MosquitoCredential wsu:Id="SecurityCredential-ABC..."
  xmlns:Credential=http://mosquito-online.org/security/Credential
  xmlns:wss=http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd
  xmlns="http://www.w3.org/2000/09/xmldsig#">
  <Credential:Header>
    <Credential:CreatedAt>2005-06-21T06:50:50Z</Credential:CreatedAt>
    <Credential:ExpiresAt>2005-06-21T14:50:50Z</Credential:ExpiresAt>
    <Credential:Issuer>Issuer XY</Credential:Issuer>
    <Credential:Holder>Holder YZ</Credential:Holder>
  </Credential:Header>
  <Credential:Attributes>
    <Credential:IdAttribute>.....</Credential:IdAttribute>
    <Credential:AuthorisationAndRolesAttribute>.....</Credential: AuthorisationAndRolesAttribute >
    <Credential:ContextInformationAttribute>.....</Credential:ContextInformationAttribute>
    <Credential:TrustAttribute>.....</Credential:TrustAttribute>
  </Credential:Attributes>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <ds:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"
        xmlns:ds="http://www.w3.org/2000/09/xmldsig#" />
      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
      <Reference URI="#SecurityCredential-ABC...">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
          <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
        <DigestValue>VSkhxcLbHxyKf/0112014oWXUM=</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>e+W7AyNmVfL6Zp8N0RJMnUr16rW+0zYT3Ae/j2d3DA7v9j.../Q3E0sTNMWC9SJjZ7tLp1JbLVomR74FKU=</SignatureValue>
  <KeyInfo>
    <wss:SecurityCredentialReference>
      <wss:KeyIdentifier ValueType="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-tok...WuQ=</wss:KeyIdentifier>
    </wss:SecurityCredentialReference>
  </KeyInfo>
</Signature>
</Credential:MosquitoCredential>

```

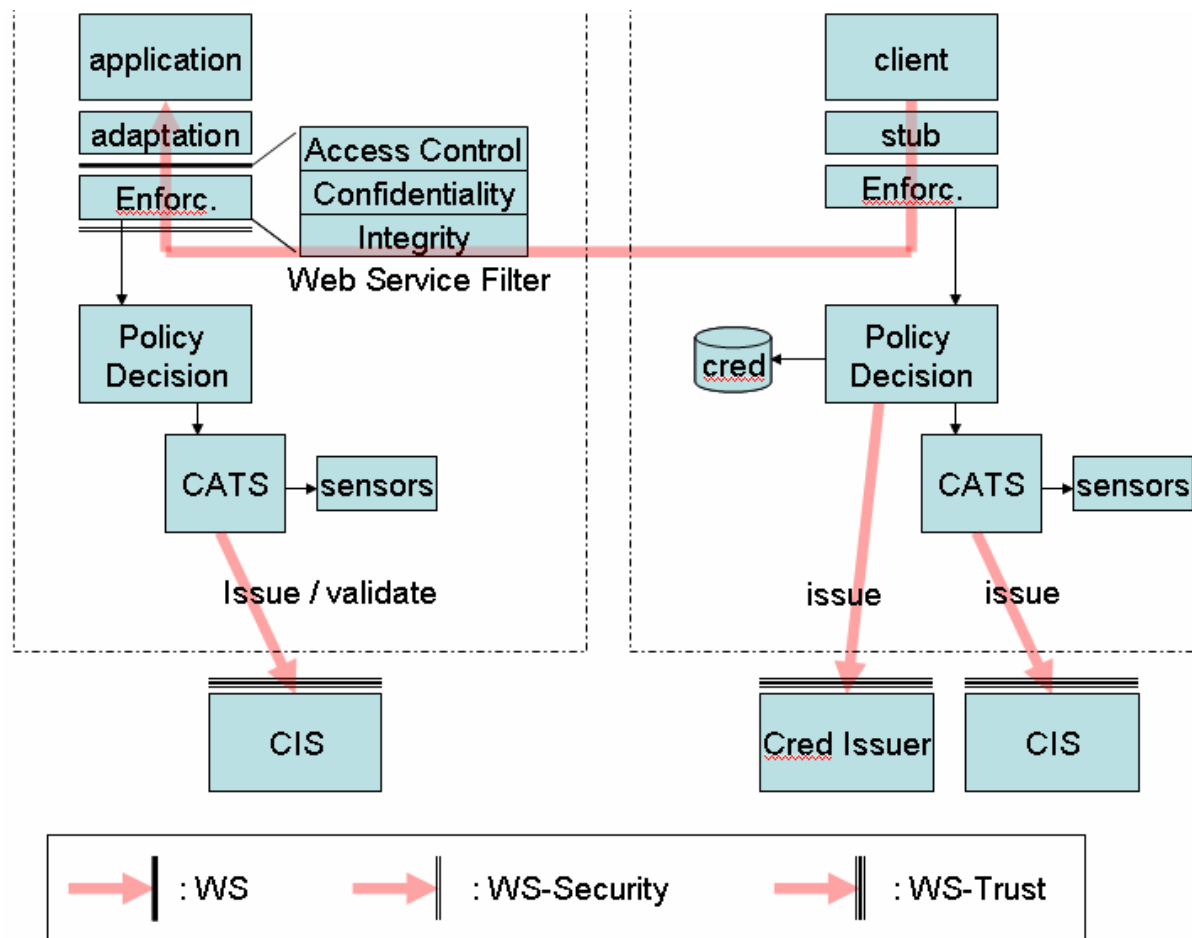


# Infrastructure

---

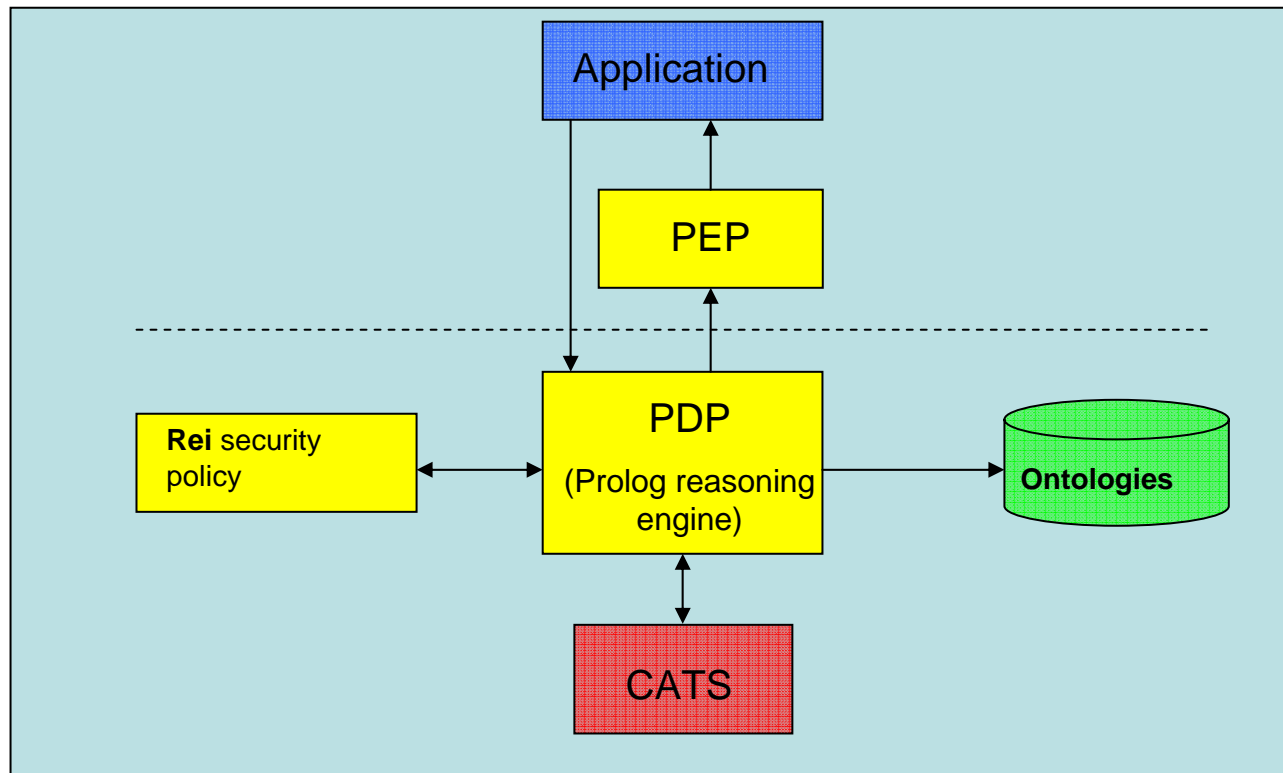
- Message level policies: web service filters
- High level policies:
  - XACML (and SAML) for access control
  - REI for other purposes
- Credentials: XML compatible with SAML and EuréCA

# Message level policies

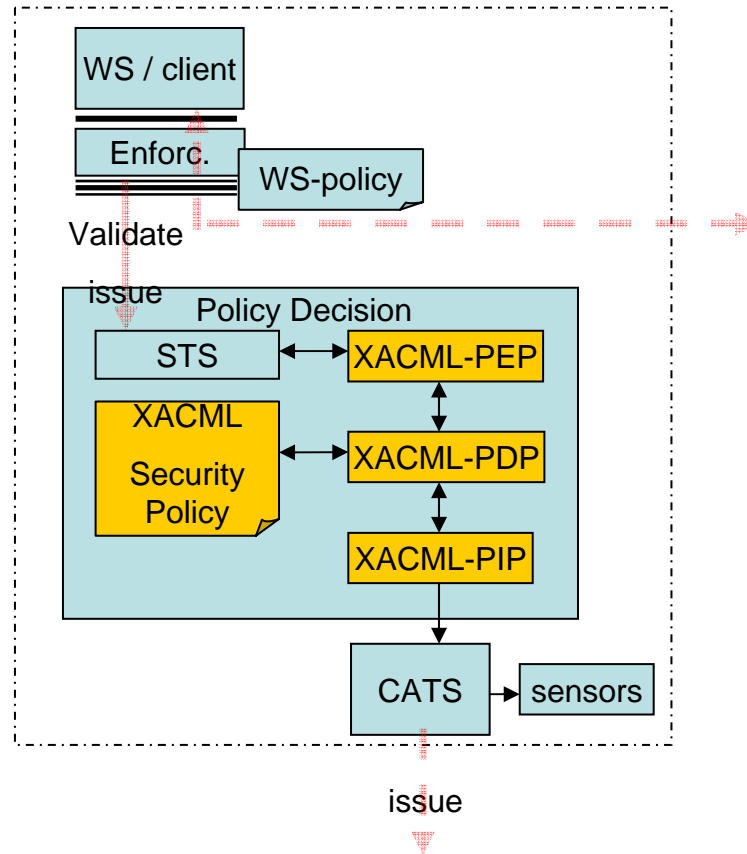


# Usage of REI in MOSQUITO

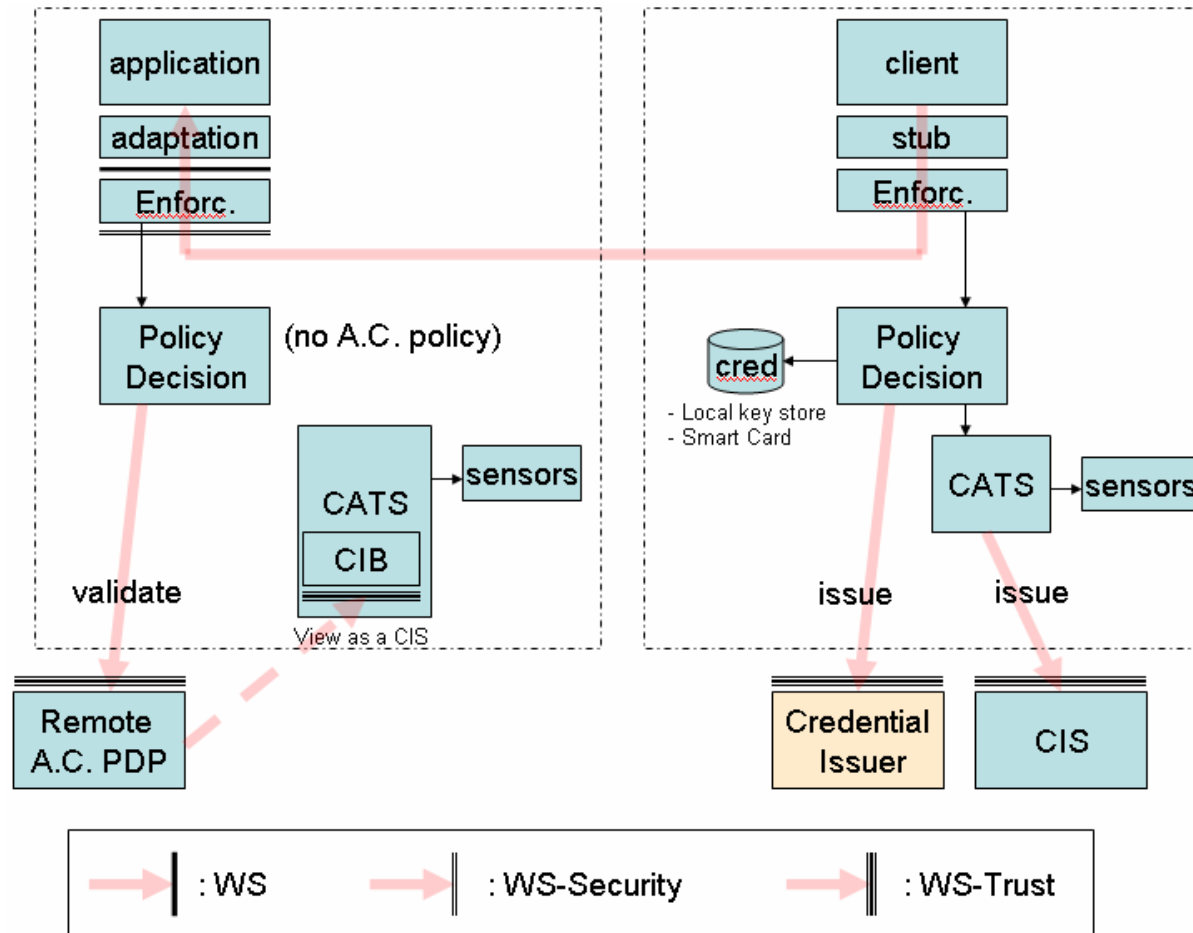
---



# XACML in MOSQUITO



# Credential request by WS-Trust



## Disclaimer

---

IST-Directorate General / Integrating and strengthening the ERA. The project MOSQUITO is supported by the European Community. This document does not represent the opinion of the European Community. It is also the sole responsibility of the author and not the responsibility of the European Community using any data that might appear therein.