

# CID identitySemantics

## Semantic Validation of Digital certificate



“Ensure that the regulatory requirements are met.

Check if the digital certificate is used for the purpose initially made by its issuers”

### Cryptographic validation

- ✓ Certificate integrity
- ✓ x.509 compliance
- ✓ Certificate issued by a validated provider

### Operacional validation

- ✓ Expiration date
- ✓ Revocation status
- ✓ Issuer Trust level
- ✓ Verifies that the certificate structure matches the policies established by the provider

### Semantic validation

- ✓ Update the validation rules and its application policy by monitoring the CSPs' policy
- ✓ Information about restrictions on the use of the certificate
- ✓ Discovery and continuous update of information that can be extracted from the certificate

It has never been that easy to integrate strong authentication using digital certificates in corporate applications. Using this tool (SOA based), it is possible to achieve a complete validation of certificate seamlessly as well as a data capture for the application that uses it.

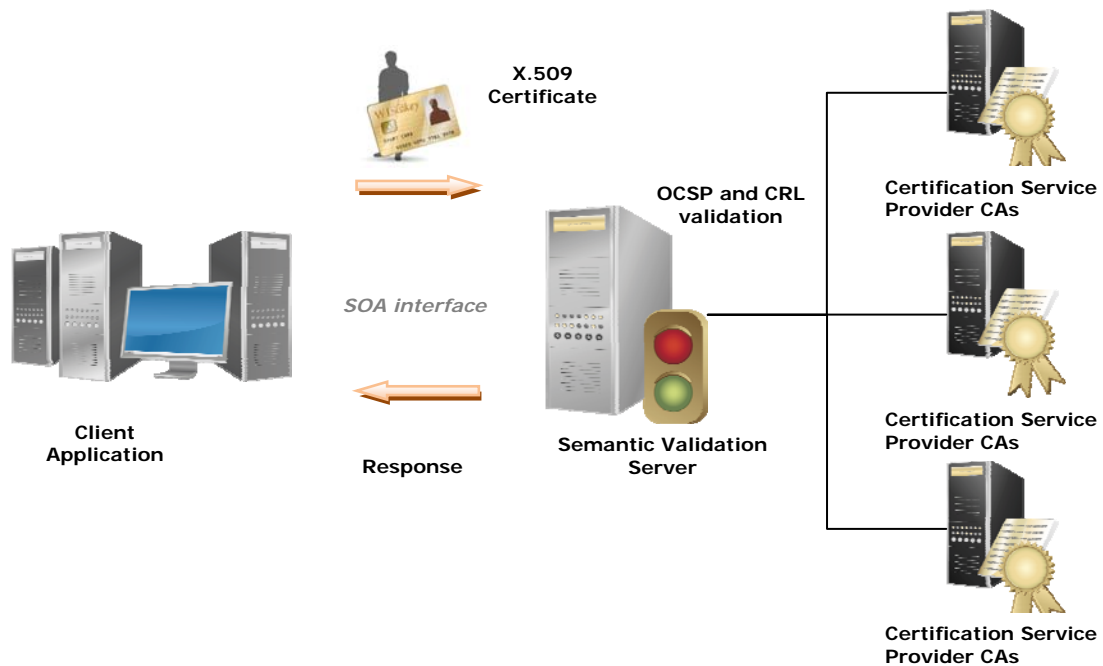
**CID identitySemantics** is a security tool designed as a service that checks the status of a digital certificate (that complies with the X.509 format) from all point of views that may concerns an application logic or business process.

Through a definition of security policy (XML template), the client establishes the following parameters:

- ∞ Certificate Service Provider (CSPs).
- ∞ Certification policy of each provider.
- ∞ Certificate usage within the information system.

In return, the response provides a full report of the status of the certificate:

- ∞ **Operational validity**
- ∞ **Cryptographic validity**
- ∞ **Legal verification**
- ∞ **Semantic information**



## Main usage

- **Securing web access:** using digital certificate to access pages or web services.
  - E-Banking.
  - Citizen portals.
  - Electronic window of services companies.
  - E-commerce....
- **Systems of qualified digital signatures:** when signing or performing a signature validation, the status of the certificate and its limitation of useage must be checked.
  - Electronic invoice.
  - Contract signature.
  - Registry of input/output.
  - Document workflow ...
- **Strong Authentication for third party applications:** secured authentication proxy based on digital certificates to integrate with basic authentication applications (user/password, etc).