

# Belgium opens e-ID electronic signature implementation

<http://ipsec.pl/node/779>

The Belgium Federal ICT Department (FedICT) is developing an eID Digital Signature Service under the GNU LGPL 3.0 open source license. The eID DSS supports the creation of XML signatures according to XAdES-X-L using a browser POST protocol to navigate the web browser from Relying Party to the eID DSS.

After verification of the to-be-signed XML document (the visualization of the XML structure can be styled using XSLT) the citizen can sign the XML structure using the eID card via the eID Applet technology. After signature finalization by the eID DSS (upgrade from XAdES-BES to XAdES-X-L using the eID Trust Service) the eID DSS will navigate the web browser back to the Relying Party where the work flow can continue.

For signature verification the Relying Party can use an eID DSS web service according to the OASIS DSS specifications. The eID DSS signature validation web service is using the eID Trust Service for historical certificate chain validation. Because both the signature creation and signature validation is outsourced to the eID DSS, the Relying Party does not need to have notion of the actual used signature format. This way the Relying Party can fully focus on the business work flow and define an XML schema according to its business needs.

Although the citizen is also offered the possibility to download the signed XML document it should be noted that the eID DSS targets integration of electronic signatures as part of a web based business work flow and is thus not document centric oriented, but service centric oriented.

Over time the eID Trust Service will support creation of trust domains using the Trusted Lists according to the Service Directive to be able to validate EU certificate chains.

e-ID DSS: <http://code.google.com/p/eid-dss/> e-ID Trust Service: <http://code.google.com/p/eid-trust-service/> e-ID Applet: <http://code.google.com/p/eid-applet/>