Ensuring secure data transmission in the BIRO infrastructure for comparing international diabetes indicators

Beck P[1], Perner P[1], Pruna S[2], Cunningham S[3], Palladino P[4], Carinci F[4]

[1] Institute of Medical Technologies and Health Management, JOANNEUM RESEARCH, Graz, Austria
[2] Institute of Diabetes, Nutrition and Metabolic disease "N. Paulescu", Bucharest, Romania
[3] Division of Medicine & Therapeutics, University of Dundee, Scotland
[4] Department of Internal Medicine, University of Perugia, Perugia, Italy

BIRO (Best Information through Regional Outcomes) is an EU/DG-SANCO funded project which aims at improving the ability to produce European diabetes indicators by defining a common infrastructure for standardized information exchange. Comparability of results is achieved by a standardized data model and a common dictionary of medical and statistical concepts. In the BIRO infrastructure, regional information systems apply standard processing to data routinely collected through regional initiatives. This processing involves calculation of 'partial' indicators consisting of aggregated data which are then transmitted to a central Shared European Diabetes Information System (SEDIS), where overall estimates are generated using meta-analytical techniques. This paper presents the BIRO infrastructure for secure data and information exchange between the regional information systems and the central SEDIS.

Based on a set of requirements (availability of an open platform-independent standard, XML support, usability over Internet protocols, availability of open source implementations and comprehensive security support), web-services were selected as the technology for implementation. That is because they use the following open World Wide Web consortium standards: SOAP (Simple Object Access Protocol) for messaging, HTTP (Hypertext Transfer Protocol) for Internet transport and XML (eXtensible Markup Language) together with its security extensions XMLenc (encryption) and XMLsig (digital signatures). The open source framework Apache Axis 2 together with Apache Rampart available for the Java 2 Enterprise Edition platform was chosen for pilot implementation. Two J2EE server applications (sender and receiver) were set up for secure data exchange using the above mentioned standards and tools. Security services (according to ISO/OSI 7498-2) were supported as follows: For authentication, digital certificates trusted by a common certification authority were exchanged and installed in both servers and access control was configured, so that only trusted identities were authorized to connect to services. Confidentiality was provided by using encryption, and data integrity as well as non-repudiation were provided by digital signatures. There were two alternative ways to apply encryption and digital signatures. On the one hand transport layer security using HTTPS, i.e. HTTP protocol together with SSL (Secure Sockets Layer) was used to protect the entire data stream exchanged between sender and receiver. On the other hand, within the SOAP messages encryption and digital signatures, utilizing XMLenc and XMLsig respectively, could be applied to protect well defined chunks of data, giving the application full control over further utilization, storage and processing of digital signatures and other security related information.

To facilitate secure data transmission in the BIRO infrastructure, an applicable technology has been selected and successfully used in a pilot implementation. This is a foundation for further integration in data exchange workflows required in a shared European diabetes information system.