ANNEX

CHAPTER 1: Exchange of DNA-Data

5. Application, security and communication architecture

5.4. Protocols and Standards to be used for encryption mechanism: s/MIME and related packages

The open standard s/MIME as extension to de facto e-mail standard SMTP will be deployed to encrypt messages containing DNA profile information. The protocol s/MIME (V3) allows signed receipts, security labels, and secure mailing lists and is layered on Cryptographic Message Syntax (CMS), an IETF specification for cryptographic protected messages. It can be used to digitally sign, digest, authenticate or encrypt any form of digital data.

The underlying certificate used by s/MIME mechanism has to be in compliance with X.509 standard. In order to ensure common standards and procedures with other Prüm applications, the processing rules for s/MIME encryption operations or to be applied under various COTS (Commercial Product of the Shelves) environments, are as follows:

— the sequence of the operations is: first encryption and then signing,
— the encryption algorithm AES (Advanced Encryption Standard) with 256 bit key length and RSA with 1 024 bit key length shall be applied for symmetric and asymmetric encryption respectively,
— the hash algorithm SHA-1 shall be applied.

s/MIME functionality is built into the vast majority of modern e-mail software packages including Outlook, Mozilla Mail as well as Netscape Communicator 4.x and inter-operates among all major e-mail software packages.

Because of s/MIME's easy integration into national IT infrastructure at all Member States' sites, it is selected as a viable mechanism to implement the communication security level. For achieving the goal ‘Proof of Concept’ in a more efficient way and reducing costs the open standard JavaMail API is however chosen for prototyping DNA data exchange. JavaMail API provides simple encryption and decryption of e-mails using s/MIME and/or OpenPGP. The intent is to provide a single, easy-to-use API for e-mail clients that want to send and received encrypted e-mail in either of the two most popular e-mail encryption formats. Therefore any state-of-the-art implementations to JavaMail API will suffice for the requirements set by Decision 2008/615/JHA, such as the product of Bouncy Castle JCE (Java Cryptographic Extension), which will be used to implement s/MIME for prototyping DNA data exchange among all Member States.