Security Rules for Transfer of Data

Customer when sending data (*i.e., data includes any type of data such as but not limited to personal data and information including confidential information*) to Gemalto's system (*i.e., set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, recording, processing or disposition of data*) or receiving data from Gemalto's system is subject to the following security rules recommended by Gemalto, Customer solely assumes all risks, liabilities and consequences if it fails to abide to such security rules:

A/ **Exchange protocol**: is in charge to protect data during their transit from and to customer premises to and from the Gemalto's system. The main objective of exchange protocol is to ensure the authentication of the parties and the integrity of the transfer.

- Recommendation: Gemalto Allynis Connect solution using secured protocols (no email).

B/ **File Encryption**: is used to protect data during their transit from Allynis Connect platform to the Gemalto's system. Recommended file encryption is based on OpenPGP standards. On top of the PGP file encryption data is transiting in a secure tunnel.

- Recommendation: PGP encryption with:

- AES - 128 bits or higher for symmetric part configuration
- RSA ≥ 3072 bits for asymmetric part configuration (key transportation)

Note: Asymmetric RSA ≥ 2048 bits and symmetric 3DES-112 bits or 3DES-168 bits are however tolerated when used with mid-term cryptographic periods.

For the implementation of the encryption it is recommended to follow NIST800-57 Part 1.

C/ **Record Encryption**: in case record encryption is available as specified by Gemalto on a case-by-case basis, it is needed to protect data until it reaches a secure safe (database or the HSM of the customer application).

- Recommandation: AES - 128 bits or higher

Note: symmetric 3DES-112 bits or 3DES-168 bits are however tolerated when used with mid-term cryptographic periods.

For the implementation of the encryption it is recommended to follow NIST800-57 Part 1.

Note: Any exception to these security rules has to be recorded in a document signed by customer and the relevant member of the Gemalto corporate group of company.