Version: 1.0 of October 28th, 2016

DATA PROCESSING TERMS FOR IN-HOUSE SOLUTION

1. Introduction:

With these provisions Gemalto desires to inform customer of the processing of data included Personal Data (as defined below) Gemalto may be accessing in providing customer with the Support Service (as defined below) covering the In-house Solution (as defined below).

2. Certain definitions

As used herein,

Back-End Components means that any component, running in the customer's premises where the In-House Solution is installed, is considered as a back-end components in the context of these data processing terms. This includes the application servers, the database servers, the underlying infrastructure components like routers, firewalls, as well as web application firewalls if they are part of the Gemalto delivery to the Customer

Client Information is personal information that Gemalto may collect from customer's employees or agents interactions with Gemalto in the provision of the Support Services.

Data Privacy Law is all laws, rules, regulations, governmental requirements, codes as well as international, federal, state, provincial laws applicable to Personal Data.

In-House Solution is Gemalto's solution for which customer is granted a license, installed in customer's premises and managed by customer.

Management System is the web base platform ticketing system known as STiM used by Gemalto in connection with the supply of the Support Service.

Personal Data is (i) data which relate to a living individual (whether in personal or family life, business or profession) who can be identified (a) from those data, or (b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, as well as (ii) information that can be utilized to identify or trace an individual's identity including but not limited to name, address, social security number, biometric data, date of birth, etc.

Remote Support is the use of telephone, email or a VPN to facilitate the resolution of a Request.

Request is a request from customer relating to the supply of the Support Service.

Request Record is a record in Management System generated by Gemalto that records and tracks Requests.

Service Data is data that resides on the In-House Solution to which Gemalto is provided access to perform the Support Services.

Service Desk is Gemalto's technical support group that acts as a single point of contact between Gemalto and customer to manage all Requests, communications and escalations with the Customer.

Support Service is the support service subject matter of an agreed upon service level agreement.

VPN is a virtual private network and provides a secure communications mechanism for data and other information transmitted between two end points.

3- **Processing of Client Information**

At the time of a Request Gemalto is collecting Client Information that is stored in the Management System located in France. The purpose of such collection is to identify the origin of the Request, associate the Request to the Customer, for the purpose of analyzing, diagnosing and resolving the Request, invoicing purpose, enhancements purpose of the In-House Solution and security.

Client Information may be transferred to the support team providing the Support Service thus triggers a cross-border transfer of data subject to the terms of Section 6 below.

4- **Remote Support**

The Support Service is provided via a Service Desk (support Level 1) located in India at SAFENET INFOTECH PVT LTD (a legal entity member of the Gemalto corporate group). The Service Desk creates a Request Record in the Management System and coordinate the response in accordance with the agreed upon service level agreement.

If the Request has to be escalated to support Level 2 the experts in charge of the support Level 2 are located at are located as specified by Gemalto in the contract/commercial offer, on a case by case basis.

If Gemalto is of the view that a Request requires a remote connection to the In-House Solution, Gemalto will connect to the In-House Solution via a secure VPN previously installed with the Customer.

Customer must provide Gemalto with access to the In-House Solution where and when needed in relation to a Request.

The remote connection to the In-House Solution is covered by the security terms set forth in Section 5 below.

If Customer has a security policy or support process that it expects Gemalto to adhere to, then Gemalto reserves the right to review the policy or process and:

a) confirms that is able to comply with it (subject to additional charge(s)); or

b) if not able to comply with it, Gemalto will not be required to adhere to the policy or process.

When remotely connected to the In-House Solution Gemalto has the ability to view and use the Service Data for the only purpose of providing the Support Service. Gemalto does not copy, modify, or delete the Service Data.

5- **Security Terms**

5.1The Support Service is following these security principles:

- only the persons needing remote access are authorized;
- only authorized actions can be performed;
- the access to the In-House Solution in done via a trustable interface;
- suspicious activities are monitored;
- actions are tracked to identify roles and responsibilities in case of investigations.

More precisely:

5.1.1 Isolation

To isolate the In-House Solution to the Gemalto infrastructure, Gemalto is proposing two solutions:

a) The first one is based on a jump server, which is blocking the direct accesses from the operators PCs to the In-House Solution. The operations can be only performed from the jump server. As the

operator hasn't the administration right of this jump server, he is only able to use authorized software already installed into the jump server;

b) The second solution is based on a dedicated infrastructure. The operator has a dedicated PC on which he has limited rights. Specific software are pre-installed on this PC to perform the maintenance and support operations. A file server is at disposal for log files transfer. An anti-virus is also installed on this dedicated PC to avoid any infection.

The goal of these two solutions is to limit as much as possible the usage of inappropriate applications and the transfer of unwilling files between the In-House Solution and the Gemalto premises.

The second aspect to this isolation is related to the bearer between the infrastructures. The communication channel has to be protected as well. For both solutions the usage of a VPN is mandatory to protect the link between the In-House Solution and the Gemalto premises.

5.1.2 Authentication

The second important aspect is the capability to authenticate the operator. This authentication has to be strong enough to avoid an identity usurpation and to be unenforceable in case of legal proceedings.

Gemalto has deployed its own system based on its two form factors authentication system. Access to the dedicated PC or to the jump server is granted with the employee personal badge. This badge is unique and embeds a private key used for this authentication.

To have an access to these systems, the operator has to present his badge and the associated PIN. The badge combined with a central LDAP (Lightweight Directory Access Protocol), provides several advantages. The first one consists to validate the badge itself. The second is allowing a group management. Based on the LDAP authentication, the system validates the operator rights accesses to the jump server and to the In-House Solution. The last point, is the easiness the access management. The newcomers' accesses and revocations management in the central system. Thanks to this strong authentication method, Gemalto guarantees that only the required persons have an access to the In-House Solution. Moreover based on the role and group definitions, the access rights are limited to the provision of Support Service.

5.1.3 Auditability

In addition with this strong authentication, the capability to do a real-time suspicious behavior detection or to perform further analysis in case of incident is doable.

The real-time detection is based on security detectors in charge to send security alerts. These alerts trig an internal process in charge to define the criticality of the detection and to launch appropriate containment actions.

The logs systems record the actions performed by the operators. Thanks the strong authentication system, the logs associate the owner and the actions.

Due to the confidentiality of certain data, logs are sanitized. These logs are stored in secure space and only security officers can have an access to them.

These combined systems allow Gemalto to detect and react in case of security alert.

5.2 Customer Acknowledgement

Customer acknowledges and understands that all the Back-End Components of the In-House Solution offered by Gemalto are intended to run on a secured and controlled environment. Such secured and controlled environment is expected to be aligned with best practices applying in each area from physical to logical security. Gemalto has elected ISO27002 standard as a proper catalog of security best practices. The In-House Solution specific security features are made available by Gemalto upon request. Customer agrees

to assume all responsibilities for failure to implement the above mentioned security features or to request the In-House Solution specific security features.

6- **Cross-Border Transfer**

6.1 As indicated in Section 4 above, the provision of the Support Service could create a cross-border transfer of Client Information and/or Support Data, customer understands that such cross-border transfer of Client Information and/or Support Data may be subject to specific requirements imposed by the applicable Data Privacy Law with the burden of such specific requirements being carried by customer as the entity making the Client Information and/or Support Data available to Gemalto.

6.2 In the event such cross-border transfer of Client Information and/or Support Data could require the entering into a specific cross-border transfer agreement in light of the applicable Data Privacy Law. Gemalto and Customer will collaborate in order to satisfy this requirement.
