CSIRT Description for GTO-CERT RFC 2350

Document Control

Approval

	Name	Date
Prepared by:	Julien VIGNOLLES	15/Sep/2016
Approved by:	Didier ESPINET	16/Sep/2016

History

Revision	Author	Date	Modification
1.0	Julien VIGNOLLES	15/Sep/2016	Initial version
1.1	Julien VIGNOLLES	06/Apr/2017	User modification, working time
1.2	Julien VIGNOLLES	15/Jun/2017	Adding pgp keys information
1.3	Julien VIGNOLLES	07/Aug/2017	Typo fixes
1.4	Julien VIGNOLLES	16/Aug/2017	Key ID update
1.5	Julien VIGNOLLES	28/Aug/2017	Typo fixes
1.6	Julien MONGENET	12/Jun/2018	Team and Roles modification

SUMMARY

1 ABOUT THIS DOCUMENT

This document contains the description of Gemalto CERT according to the RFC 2350. It provides information about Gemalto CERT Team, communication channel and services.

1.1 Date of Last Update

This is the v1.6 version released on June, 12th 2018

1.2 Distribution List for Notifications

Distribution List for notifications changes related to this document are not distributed by a Mailing List, or any other mechanisms.

1.3 Location where this Document May be Found

The current version of this Gemalto CERT description is available on PDF format on the Gemalto website.

http://www.gemalto.com/csirt-site/Documents/GTO-CERT_RFC2350.pdf

1.4 Authenticating this Document

These documents have been signed with the GTO-CERT PGP key. The signatures are available on our website, under:

http://www.gemalto.com/csirt

2 CONTACT INFORMATION

2.1 Name of the Team

The registered name of the team is **Gemalto CERT** and the acronym is "**GTO-CERT**".

2.2 Address

Gemalto S.A.

CSIRT – PO 63

525 Avenue du Pic de Bertagne – BP100

13881 GEMENOS Cedex – France

2.3 Date of Establishment

Gemalto CERT was established on October 2013

2.4 Time Zone

CET/CEST : Europe/Paris (GMT+01:00, and GMT+02:00 on DST)

2.5 Telephone Number

+33 4 42 36 50 00 (Standard ask for CSIRT Team)

2.6 Facsimile Number

+33 4 42 36 42 00

2.7 Other Telecommunication

None available

2.8 Electronic Email Address

All incident reports should be submitted to <csirt(at)gemalto.com>

2.9 Public Keys and Other encryption Information

GTO-CERT PGP Key information are:

KeyID: 0x22F798E9

Fingerprint: 4F70 146C 5D16 A1F8 E0D9 F0BB 1654 DDAC 22F7 98E9

The public key and its signature can be found at the usual large public key servers, or on Gemalto CERT information page: http://www.gemalto.com/csirt-site/Documents/CSIRT.ASC

2.10 Team Members

CERT Coordination is performed by Julien Mongenet. All team members contact information are listed below:

Name	*Email Address*	*Key ID*	*Role*
Didier Espinet	didier.espinet(at)gemalto.com	0x88DDFC96	Representative
	Fingerprint	B9B3E19CFD054FE00A6B6C3A0F7071F188DDFC96	
Julien Mongenet	julien.mongenet(at)gemalto.com	0xE669D123	Coordinator
	Fingerprint	E9B6843354E48DCDC79E6EE610675DCAE669D123	
Rita Barakat	rita.barakat(at)gemalto.com	0xF5784E24	Core Team
	Fingerprint	A4755BE33699F74F4A3122E4F76D4849F5784E24	
Sebastien Schmitt	sebastien.schmitt(at)gemalto.com	0xDA99C12F	Core Team
	Fingerprint	02631D7C110D4855A0AFA56FED6EAC8FDA99C12F	

2.11 Points of Customer Contact

In case of security incident, in addition of regular Gemalto point of contact (Sales, support team), customers could submit incident report to <csirt(at)gemalto.com>.

3 CHARTER

3.1 Mission Statement

The Gemalto CERT Team's activities are non-profit and fully financed by Gemalto S.A. The purpose of Gemalto CERT are to:

- Handle, contain, investigate and resolve serious computer security incident which can affect Gemalto's assets and interests including Gemalto's Customers, Employees, Partners and Shareholders, according the laws and regulations that may apply.
- Prevent and anticipate Computer Security Incidents by implementing adequate processes, tools, policies to improve the reactivity in case of an incident.
- Supports at a corporate level the crisis cell and manage the security implication of a crisis
- Provide information, expertise, assistance and tools to Gemalto to proactively reduce the risk of such incidents.

3.2 Constituency

The Gemalto CERT organization is divided into four constituencies: Infrastructure Technology, Operated Services, Manufacturing and Corporate Security, with all necessary Incident Response and Management activities. Gemalto CERT aims at providing cyber security expertise, defense, and efficient reactivity to protect our customers, shareholders and employees.

3.3 Sponsorship and/or affiliation

Gemalto CERT is a private CERT in the industrial sector. It is owned, operated and financed by Gemalto S.A

It maintains relationships with different CSIRTs in France and in Europe.

Gemalto CERT is registered on Trusted Introducer since October 2016

https://www.trusted-introducer.org/directory/teams/gto-cert.html

3.4 Authority

Gemalto CERT operated under the auspices of, and with the authority delegated by the Chief Security Officer of Gemalto. GTO-CERT strives to work cooperatively with IT Managers, System Administrators, SOC, Datacenter Security Officer, Solution Security Officer and Security Site Managers to avoid authoritarian relationship whenever possible. However, under circumstances, Gemalto CERT will appeal to CIO, (S)VP, EVP to exert its authority directly or indirectly.

4 POLICIES

4.1 Types of Incidents and Level of Support

Gemalto CERT manages all types of computer security incident which occur, or threaten to occur, in the different constituencies mentioned above. All confirmed incidents are qualified by type of incident and severity (Low, Medium, and High) according to our severity matrix. In all cases responses will be made according the priority and severity of incident reported.

Note that no direct support is given to end users; they are expected to contact their Service Desk or Local IT Managers, Security Site Managers for assistance.

4.2 Co-operation, Interaction and Disclosure of Information

Gemalto CERT develops and maintain communication channels with other CSIRTs through official communication ways and specific tools (MISP).

GTO-CERT protects sensitive information (business, privacy) in accordance with relevant law and regulations that may apply of the different countries where Gemalto is present.

GTO-CERT applies Light Traffic Protocol (TLP) when sharing information with team that support it. TLP classification is based on the global Gemalto Document Classification Policy.

4.3 Communication and Authentication

In view of the types of information that GTO-CERT deal with, telephone will be considered sufficiently secure to be used even unencrypted. However, GTO-CERT will refrain exchanging too sensitive detailed information through telephone and ask counterparts to proceed with encrypted emails.

Unencrypted e-mail must be used to submit non-sensitive information, and will not be considered as secure.

To submit high-sensitive data we encourage the use of the encryption means such as PGP Key (external) or X.509 cryptography for internal e-mail. PGP key information is described above.

All external e-mail coming from Gemalto CERT is digitally signed PGP or X.509

5 SERVICES

5.1 Incident Response

GTO-CERT is informed about all security incident that occurs in the different constituencies. According to the extent of the security incident, GTO-CERT takeover the lead and manage containment, analysis and recommend remediation actions with the support of system administrators and business managers.

5.1.1 Incident Triage

- Confirm If the security event report is a relevant security incident
- Perform quick assessment (type, constituency, severity) of security incident confirmed and escalated incident

5.1.2 Incident Coordination

- Determine the priority of the incident
- Take and push to constituency affected a first level of containment
- Manage the incident on GTO-CERT side (investigations, reporting) and liaise with local security actors
- Communicate with other external parties if relevant
- Publish internal bulletin (Security Alert, Vulnerability information) to security coordinators & actors within the different constituencies.
- Attend to crisis meeting and liaise with legal, communication and business for technical security investigation that are in progress

5.1.3 Incident Resolution

- Lead technical investigation, this could be done by local people but reported to CSIRT Core Team.
- Provision IOCs and liaise with SOC Team to detect and block abnormal activities
- Tune first level of containment according to the extent of the incident
- Determine the root causes and request Fix/Patch/Hardening of the affected systems
- Collect and store evidences, to start legal actions if necessary.
- Follow remediation and recovery activities until security risk dropdowns.
- Recommend security improvements to system administrators and business managers (Post-Mortem)

5.2 Proactive Activities

Regarding GTO-CERT resources, we coordinate and maintain the following services

- Threat notification
- Cybersecurity support and advices
- Vulnerability survey tool
- Training and educational services

6 INCIDENT REPORTING FORMS

To ease security event reports (Incident, Vulnerability), you can directly sent an email to <csirt(at)gemalto.com> with an explicit subject describing the issue encountered. In addition, for emergency notification, we encourage you to prefix your email's subject with [URGENT]. According to the sensitivity of the information, prefer to cipher and digitally sign your email.

7 DISCLAIMERS

While every precaution will be taken in the preparation of information, notifications and alerts, Gemalto S.A. assumes no responsibility for errors or omissions, or for damages.

END OF DOCUMENT