# CERT-Amossys

# RFC 2350

## *Description du CERT-Amossys selon la RFC 2350*


**Reference: CERT-Amossys-RFC2350-FR-1.10**

**Date: 19/10/2022**

# SOMMAIRE

# 1. Description du document

Ce document représente une description du ***CERT-AMOSSYS***, au sens de la RFC 2350[1]. Il fournit des informations de base sur le ***CERT-AMOSSYS***, décrit ses responsabilités et missions ainsi que ses moyens de communication.

## 1.1. Date de mise à jour

Version 1.01, publiée le 19/10/2022.

## 1.2. Liste de diffusion des notifications

Il n'existe pas de liste de diffusion des notifications pour les modifications de ce document.

## 1.3. Lieux de distribution de ce document

La version courante et à jour de ce document peut être retrouvée sur la page Web du ***CERT-AMOSSYS*** : https://www.amossys.fr/fr/urgence-cert-amossys/.

## 1.4. Authentifier ce document

Ce document a été signé par la clé PGP du ***CERT-AMOSSYS***.

La clé PGP, son ID et son empreinte sont disponibles sur le site Web du ***CERT-AMOSSYS*** : https://www.amossys.fr/fr/urgence-cert-amossys/.

## 1.5. Identification du document

| | |
|---|---|
| Titre | CERT-Amossys-RFC-2350-FR |
| Version | 1.10 |
| Date du document | 19/10/2022 |
| Expiration | Ce document est valide jusqu'à la publication d'une nouvelle version. |

[1] http://www.ietf.org/rfc/rfc2350.txt

# 2. Informations de contact

## 2.1. Nom de l'équipe

Le nom de l'équipe est « ***CERT-AMOSSYS*** ».

## 2.2. Addresse

Immeuble Le Ouessant
Bâtiment B
11, rue Maurice Fabre
35000 Rennes - France

## 2.3. Zone horaire

Central European [Summer] Time (CET/CEST).

## 2.4. Numéros de téléphone

Les numéros de téléphone principaux du ***CERT-AMOSSYS*** sont :

- 07 62 62 44 98
- 06 99 05 62 34

La ligne principale d'***AMOSSYS*** est 02 99 23 15 79.

## 2.5. Numéro de fax

*Non applicable.*

## 2.6. Autres moyens de communication

*Non applicable.*

## 2.7. Adresse email

L'adresse email du ***CERT-AMOSSYS*** est cert@amossys.fr.

## 2.8. Clés publiques et informations de chiffrement

PGP peut être utilisé pour les échanges avec le ***CERT-AMOSSYS***.

| | |
|---|---|
| ID utilisateur | CERT-Amossys <cert@amossys.fr> |
| ID de clé | 0x4838 736B |
| Empreinte | 52EA CDBF F028 14D5 0013 5C0D A15B B709 4838 736B |

La clé publique est disponible sur https://www.amossys.fr/fr/urgence-cert-amossys/cle-publique/.

Elle peut également être téléchargée depuis les serveurs PGP courants.

## 2.9. Membres de l'équipe

La liste des membres du ***CERT-AMOSSYS*** n'est pas disponible publiquement.

## 2.10. Autres informations

Visitez notre site Web pour plus d'informations :

- Présentation du ***CERT-AMOSSYS*** : https://www.amossys.fr/fr/nos-prestations/cert/
- Page de contact du ***CERT-AMOSSYS*** : https://www.amossys.fr/fr/urgence-cert-amossys/

## 2.11. Points de contact des clients

La méthode principale pour contacter le ***CERT-AMOSSYS*** est le téléphone. L'alternative est le mail cert@amossys.fr. Si vous nécessitez une assistance d'urgence, un appel à l'un des numéros de téléphone ci-dessus pourrait être plus rapide (voir §2.4).

# 3. Charte

## 3.1. Ordre de mission

L'objectif du ***CERT-AMOSSYS*** est d'assister ses clients lorsque des investigations numériques sont requises, ou lorsqu'un incident de sécurité survient sur leur SI.

## 3.2. Périmètre d'intervention

Les activités du ***CERT-AMOSSYS*** sont réalisées pour ses clients qui nécessitent des investigations numériques.

## 3.3. Support ou relations

Le ***CERT-AMOSSYS*** est un CSIRT commercial, mis en place, possédé et opéré par la société ***AMOSSYS***.

Des contacts sont établis avec plusieurs CSIRTs en France et en Europe, selon les besoins.

## 3.4. Autorité

Le ***CERT-AMOSSYS*** opère dans le cadre de contrats, validés et signés avec ses clients. L'équipe n'a aucune autorité pour demander la réalisation d'actions sur les systèmes et réseaux sur les périmètres impactés.

# 4. Politique

## 4.1. Types d'incidents et niveau d'assistance

Le ***CERT-AMOSSYS*** est en mesure de traiter tous les types d'investigation numérique et d'incidents de sécurité qui peuvent impacter, ou menacer, ses clients.

Le niveau de service founi par le ***CERT-AMOSSYS*** peut varier, selon les contrats mis en place entre ***AMOSSYS*** et ses clients.

Les services proposés par le ***CERT-AMOSSYS*** incluent des services de réaction et de prévention :

- Prise en compte des incidents en 24 heures ;
- Inforensique et analyse d'incidents ;
- Assistance et support à la réponse à incident ;
- Réponse à incident et remédiation ;
- Analyse de vulnérabilités et de codes malveillants.

## 4.2. Cooperation, intéractions et diffusion d'informations

Les politiques d'échanges d'informations du ***CERT-AMOSSYS*** ont été définis de façon à :

- être en conformité avec :
  - la loi Française ;
  - les besoins de confidentialité de ses clients ;
- bénéficier des avantages de la coopération avec la communauté des CSIRTs.

Toute information reçue par le ***CERT-AMOSSYS*** est considérée confidentielle par défaut, et manipulée en conséquence. Seuls les membres du ***CERT-AMOSSYS*** disposant du besoin d'en connaître pourront avoir accès à ces données, soit :

- les membres de l'équipe assignée à l'investigation ;
- les Directeur et Responsable du ***CERT-AMOSSYS*** (pour la gestion des projets).

Après chaque investigation, le ***CERT-AMOSSYS*** se réserve la possibilité de demander l'autorisation formelle du client concerné pour partager certains constats ou données techniques en lien avec l'investigation avec la communauté. Ce partage d'information peut être refusé par les clients et est réalisé, le cas échéant, avec les principes du besoin d'en connaître (toutes les informations partagées sont anonymisées et les informations sur la victime de l'incident ou son contexte sont supprimées). Si le client l'autorise, le ***CERT-AMOSSYS*** pourra partager librement les informations demandées avec la communauté, lorsque nécessaire.

Toutes les données sensibles (telles que données personnelles, configuration des systèmes, vulnérabilités, etc.) seront transmises de manière chiffrée lorsque cette transmission sera réalisée sur des canaux non protégés (voir le paragraphe suivant). Il est également recommandé aux clients du ***CERT-AMOSSYS***, lorsqu'ils échangent des données sensibles, de le mentionner explicitement. Les échanges possédant des marquages conformes au protocole ISTLP seront ainsi traités en conséquence.

Enfin, tous les membres du ***CERT-AMOSSYS*** ont signé la charte d'éthique applicable aux activités du ***CERT-AMOSSYS.***

## 4.3. Communication et authentification

Au vu des informations que le ***CERT-AMOSSYS*** peut être amené à manipuler, les communications par téléphone sont considérées suffisamment sécurisées, même si celle-ci ne sont pas chiffrées. Les échanges par emails non chiffrés ne sont pas considérés sécurisés, néanmoins ils sont suffisants pour la transmission d'informations non sensibles.

Si l'échange de données sensibles doit être effectué par email, le chiffrement de ceux-ci (par exemple par PGP) doit être mis en place (voir §2.8).

Toutes les communications provenant du ***CERT-AMOSSYS*** sont signés numériquement au moyen de la clé PGP mentionnée précédemment, ou au moyen de la clé des membres du ***CERT-AMOSSYS*** impliqués dans l'investigation.

S'il est nécessaire d'établir un canal de confiance, par exemple avant d'échanger des informations sensibles, l'identité des parties pourra être authentifiée par tout moyen légal suffisant.

# 5. Prestations et services

## 5.1. Réponse à incident

Le ***CERT-AMOSSYS*** assiste les équipes de gestion des systèmes d'information, ou de gestion de la sécurité des SI, dans la gestion des aspects techniques et organisationnels des incidents de sécurité. En particulier, le ***CERT-AMOSSYS*** peut apporter une assistance ou des conseils dans différents domaines de la réponse à incidents.

## 5.2. Gestion d'incident

- Evaluation de la gravité des incidents. Premier niveau de réponse ;
- Si nécessaire, escalade au responsable du CERT. Deuxième niveau de réponse ;
- Si nécessaire, escalade au directeur du CERT.

## 5.3. Coordination de la gestion d'incident

- Catégorisation des informations reliées à l'incident, en fonction de leur niveau de protection ;
- Communication des rapports d'incidents aux équipes techniques et managériales de la victime, en fonction de leur niveau d'expertise ;
- Coordination des analystes et des experts techniques de la victime ;
- Accompagnement pour les contacts avec les autorités judiciaires, si nécessaire.

## 5.4. Investigation et remédiation

- Analyse des systèmes compromis ;
- Conseils et accompagnement pour la suppression des vulnérabilités ;
- Conseils et accompagnement pour le durcissement des SI suite à l'incident ;
- Evaluation de la possibilité, pour les actions de collecte et d'analyse, à endommager ou altérer les preuves, en fonction de leur coût et de leur risque (collecte de preuves, observation d'un incident en cours, positionnement de pièges pour les attaquants, etc.).

## 5.5. Prestations proactives

- Audits de sécurité des SI (pentest, audits organisationnels, etc.) ;
- Recherche de compromissions / *threat hunting*. Les équipes du ***CERT-AMOSSYS*** peuvent conduire des investigations sur des réseaux ou systèmes, afin de rechercher des potentiels compromissions de ceux-ci.

# 6. Formulaire de remontée d'incident

Aucun formalisme n'est requis pour la remontée d'incidents de sécurité, néanmoins il est recommandé de fournir, dès la première communication, les informations de base sur l'incident (quoi ? quand ? qui ? comment ?) et les premières hypothèses formulées par la victime.

*Fin du document*