

**PROCÉDURE SDI SECNUM
N° 2329**

**Emploi du logiciel et des clefs ACID Cryptofiler
par une personne morale externe à la DGA**

Édition 1.1

(Les dates précises d'approbation et de publication sont accessibles dans SysMan)



**L'édition en vigueur de ce document est celle accessible dans SysMan,
avec les informations complémentaires de sa fiche documentaire dématérialisée.
S'assurer de la validité et de la complétude de toute copie avant usage.**

Rédaction	SSDI/CSDI/CRPA	Spécialiste chiffre confirmé
Vérification	SSDI/CSDI/CRPA	Chef du CRPA
Vérification	SSDI/CSDI	Chef du CSDI
Vérification	SSDI/DOCS	Animatrice du sous-domaine SecNum
Vérification	SSDI/DOCS	Responsable du sous-domaine SecNum
Validation	SSDI/AD	Responsable délégué du domaine SDI
Approbation	SSDI/D	Responsable du domaine SDI

POSITIONNEMENT DANS L'ENVIRONNEMENT DGA

Directions (entités) d'application :	Personnes morales hors et en relation avec la DGA
Activité du domaine de performance :	SDI SecNum 3
Pôles/métier :	MRC / SDI
Systèmes de management :	ISO 9001

EVOLUTIONS

Nature des évolutions :	Mise à jour des adresses emails
Documents abrogés par cette édition :	Procédure SDI SECNUM N°2329 1 ^{er} édition

DÉCLINAISON

Autorisation de déclinaison :	<input type="checkbox"/>	Le cas échéant, précisions du périmètre de déclinaison :

TABLE DES MATIÈRES

1. OBJET DU DOCUMENT	4
2. CHAMP D'APPLICATION	4
3. SIGLES ET ABREVIATIONS.....	5
4. LOGIGRAMME.....	5
4.1 OBTENTION DU LOGICIEL AVEC LA BIBLIOTHEQUE FR	5
4.2 OBTENTION DU LOGICIEL AVEC LA/LES BIBLIOTHEQUE(S) UE OU OTAN	5
4.3 DEMANDE DE CLE ACID FR	6
4.4 DEMANDE DE CLE ACID UE OU OTAN	6
5. OBJECTIFS DE LA SOLUTION DE SECURITE ACID	7
6. LES BIBLIOTHEQUES CRYPTOGRAPHIQUES.....	7
6.1 FR	7
6.2 UE	7
6.3 OTAN	7
7. CLE ACID 8	
8. LES REGLES DE SECURITE	8
8.1 HOMOLOGATION	8
8.2 NOMADISME.....	8
8.3 LE CORRESPONDANT ACID	9
9. OBTENTION DU LOGICIEL ACID CRYPTOFLER	9
9.1 ACCES A LA BIBLIOTHEQUE FR	9
9.2 ACCES AUX BIBLIOTHEQUES UE ET OTAN	10
10. OBTENTION DES CLES ACID	10
11. RENOUELEMENT DES CLES	11
12. CESSATION DE FONCTION D'UN COLLABORATEUR.....	11
13. COMPROMISSION D'UNE CLE PRIVEE OU DU MOT DE PASSE.....	12
14. ENREGISTREMENTS	13

PROCÉDURE

Objet : Emploi du logiciel et des clefs ACID Cryptofiler par une personne morale externe à la DGA

Références¹ :

- [REF A] Instruction générale interministérielle 1300 du 09 août 2021 portant sur la protection du secret de la défense nationale
- [REF B] Instruction ministérielle 900 du 15 mars 2021 relative à la protection du secret et des informations diffusion restreinte et sensibles
- [REF C] Instruction interministérielle 901 du 28 janvier 2015 relative à la protection des systèmes d'informations sensibles
- [REF D] Doctrine d'emploi et de diffusion du logiciel ACID CRYPTOFILERS, Note N°2609/ANSSI/SDE/PSS/BQA/DR-DF du 26 juin 2014
- [REF E] Instruction technique d'emploi ACID, Note N°D-21-003170/ARM/EMA/COMCYBER/DR du 14 juin 2021

1. OBJET DU DOCUMENT

Le présent document a pour objet de préciser les modalités d'exploitation et d'installation du logiciel ACID Cryptofiler délivré par la Direction Générale de l'Armement (DGA) aux EPA (établissement public administratif) et EPIC (établissement public industriel et commercial) sous tutelle de la DGA ou aux entités de droit privé dans le cadre des opérations d'armement, des projets et des marchés de la DGA pour les échanges d'informations protégées DIFFUSION RESTREINTE (DR), RESTREINT UE et RESTREINT OTAN.

2. CHAMP D'APPLICATION

Les termes du présent document s'appliquent aux entités de droit privé ou étatiques ayant obtenu ACID Cryptofiler auprès de la DGA.

Ces entités doivent assurer la protection des informations sensibles jusqu'au niveau DIFFUSION RESTREINTE, RESTREINT UE ou RESTREINT OTAN, conformément aux textes de [REF A], [REF B] et [REF C], notamment dans le cas des transmissions électroniques transitant sur des réseaux non protégés.

Les informations à protéger doivent être chiffrées à l'aide de produits de sécurité agréés, qualifiés ou certifiés par l'ANSSI.

Le produit ACID Cryptofiler est soumis à une démarche de qualification au niveau standard conduisant à un agrément de l'ANSSI et permettant de répondre à toutes ces exigences.

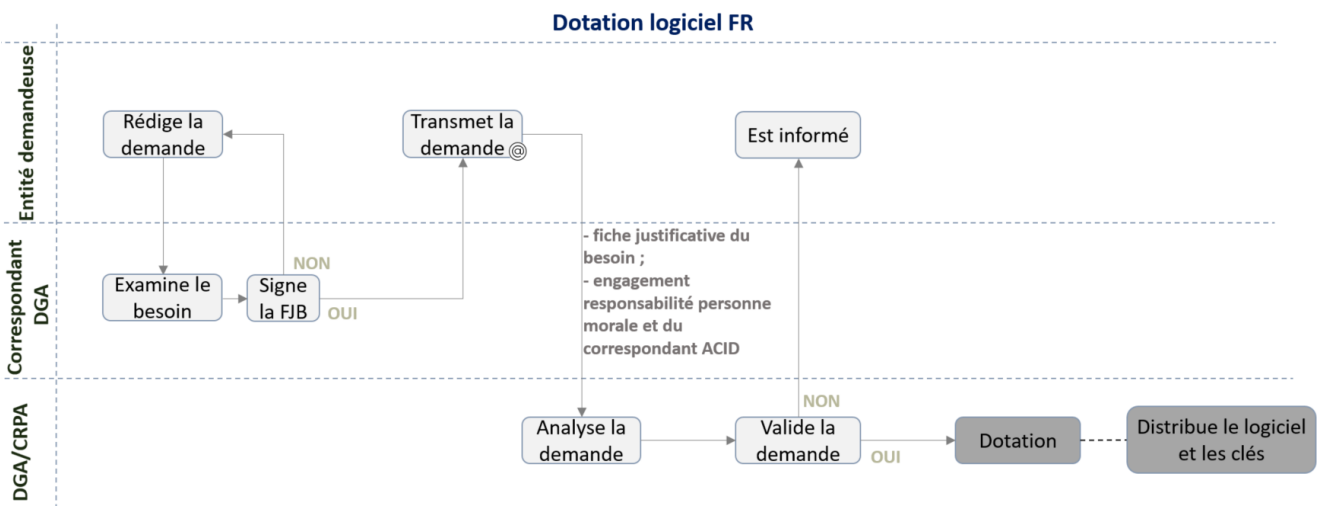
¹ Les documents [REF D] et [REF E] ne sont pas diffusables.

3. SIGLES ET ABREVIATIONS

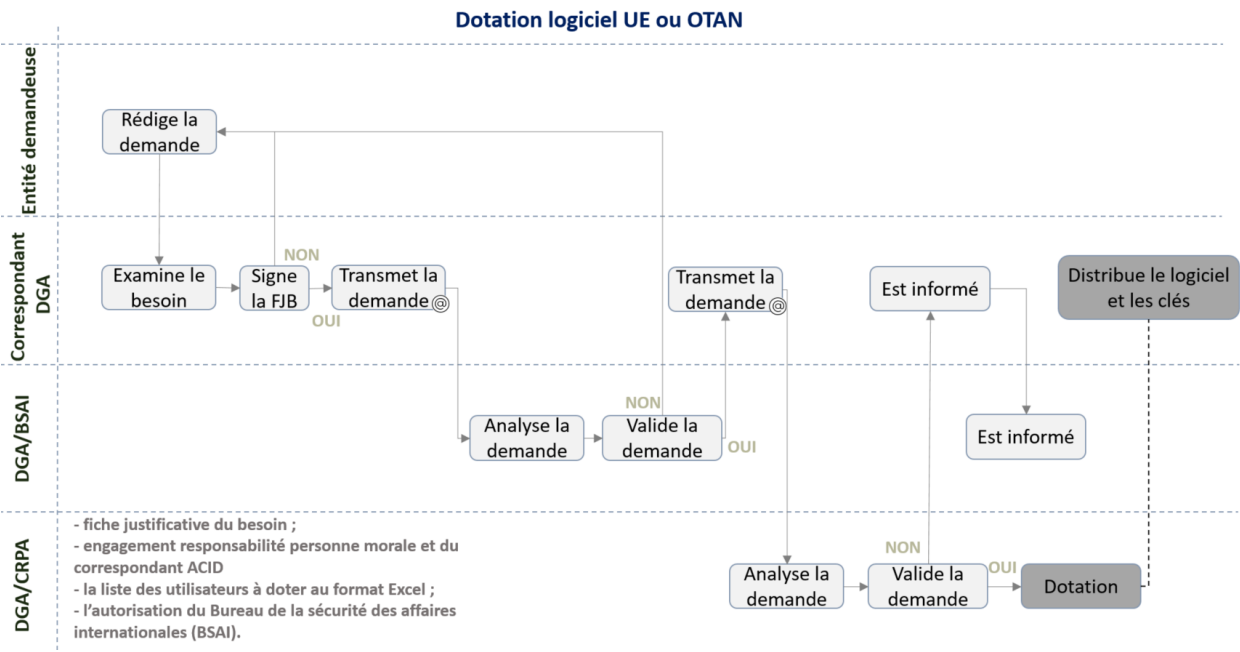
BSAI	Bureau de la sécurité des affaires internationales (au sein du SSDI)
CRI	Compte Rendu d'Incident
CRPA	Commandement des Réseaux Particuliers de l'Armement
DR	Diffusion Restreinte (mention de protection)
FJB	Fiche Justificative du Besoin
ISO 9001	Norme à exigences relatives au système de management de la qualité de l'organisme
MinArm	Ministère des Armées
OTAN	Organisation du Traité de l'Atlantique Nord
PCS	Plan Contractuel de Sécurité
PES	Procédures d'Exploitation et de Sécurité
SDI	Sécurité de Défense et de l'Information
SecNum	Sécurité du Numérique
SF	Spécial France (mention complémentaire de protection)
SSDI	Service de la sécurité de Défense et des systèmes d'Information
UE	Union Européenne

4. LOGIGRAMME

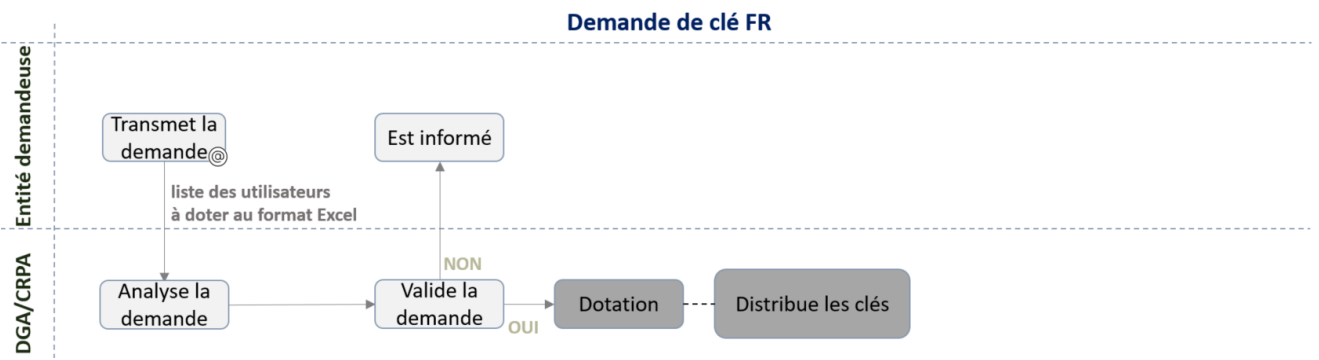
4.1 OBTENTION DU LOGICIEL AVEC LA BIBLIOTHEQUE FR



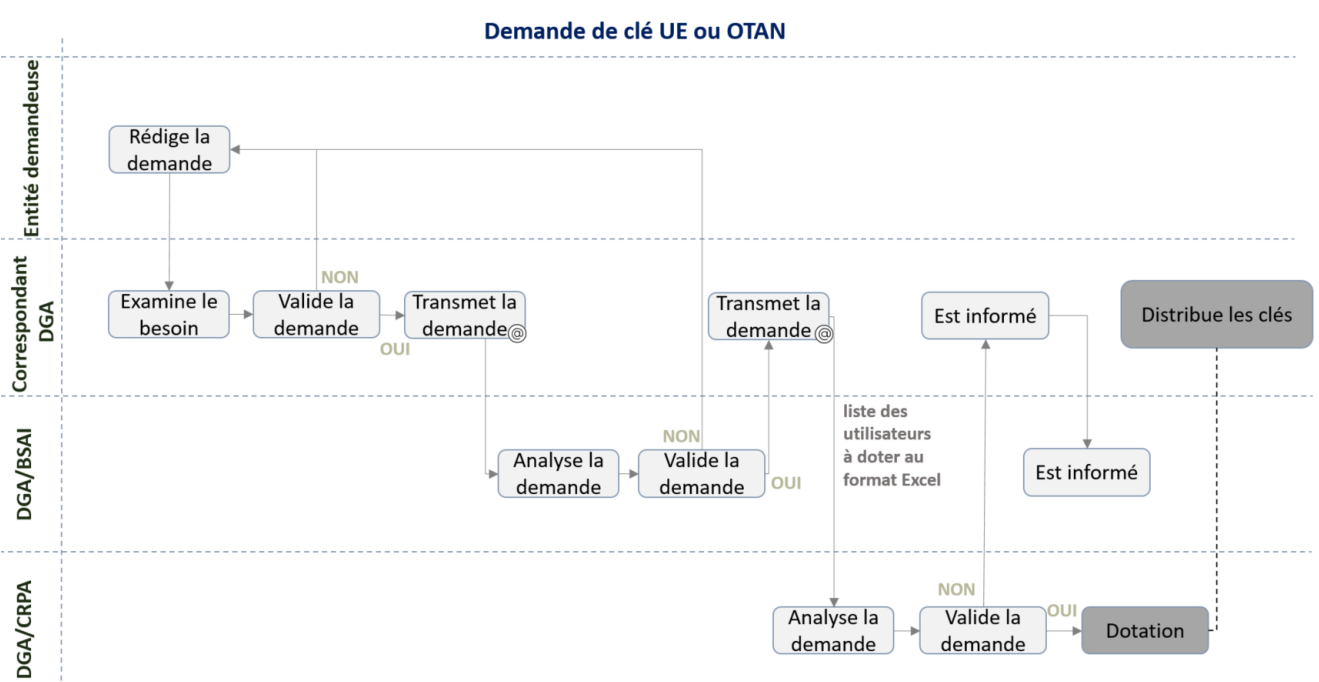
4.2 OBTENTION DU LOGICIEL AVEC LA/LES BIBLIOTHEQUE(S) UE ou OTAN



4.3 DEMANDE DE CLE ACID FR



4.4 DEMANDE DE CLE ACID UE ou OTAN



5. OBJECTIFS DE LA SOLUTION DE SECURITE ACID

La solution ACID Cryptofiler permet la protection d'informations sensibles jusqu'au niveau DIFFUSION RESTREINTE ou portant une mention de manipulation. Elle permet également la protection d'informations de niveaux « Restreint » de l'OTAN et l'UE.

ACID Cryptofiler permet :

- une protection des informations sensibles en offrant le chiffrement de fichiers regroupés dans des conteneurs² ;
- un service de contrôle de l'intégrité et de l'origine des informations par la signature de fichiers regroupés dans des conteneurs ;
- un effacement sécurisé ;
- un chiffrement de volumes à la volée (ACID-Disk).

6. LES BIBLIOTHEQUES CRYPTOGRAPHIQUES

Le logiciel ACID Cryptofiler dispose de trois bibliothèques cryptographiques : France (FR), Union Européenne (UE) et Organisation du traité de l'Atlantique nord (OTAN).

6.1 FR

La bibliothèque FR permet d'échanger des informations nationales jusqu'à DR. Elle doit être installée sur des postes de travail Windows appartenant à un périmètre d'homologation DR³, administrés par des personnels Français appartenant à une entreprise ou un organisme français et exploités par des personnels de nationalité française.

6.2 UE

La bibliothèque UE permet d'échanger des informations RESTREINT UE maximum. Elle peut être installée sur les postes de travail répondant à l'une des caractéristiques suivantes :

- déjà autorisés pour l'installation de la bibliothèque FR ;

ou

- homologués au minimum au niveau RESTREINT UE, administrés par des personnels de nationalité d'un pays membre de l'UE, appartenant à un organisme ou une entreprise européenne et exploités par des personnels de nationalité d'un pays membre de l'UE.

6.3 OTAN

La bibliothèque OTAN permet d'échanger des informations RESTREINT OTAN maximum. Elle peut être installée sur les postes de travail répondant à l'une des caractéristiques suivantes :

- déjà autorisés pour l'installation de la bibliothèque FR ;

ou

- homologués au minimum au niveau RESTREINT OTAN, administrés par des personnels de nationalité d'un pays membre de l'OTAN, appartenant à un organisme ou une entreprise européenne et exploités par des personnels de nationalité d'un pays membre de l'OTAN.

² Aussi appelés « archives » dans le logiciel

³ ACID Cryptofiler peut également être utilisé sur un SI SECRET (S) ou TRES SECRET (TS) afin de limiter le droit d'en connaître

7. CLE ACID

La clé ACID, dite clé « privée » ou « rouge », est protégée par un mot de passe. Elle permet également la génération d'une clé dite « publique » ou « bleue ».

La clé privée et le mot de passe sont strictement personnels, **il est donc interdit les diffuser à une tierce personne**. La clé publique, quant à elle, peut être transmise par voie numérique en clair. Le mot de passe doit être robuste et modifié dès l'installation.

De plus, l'attribution des clés ACID à un utilisateur devra respecter les conditions suivantes :

Bibliothèque	Nationalité de l'utilisateur
FR	Française
UE	D'un pays membre de l'Union Européenne
OTAN	D'un pays membre de l'OTAN ⁴

8. LES REGLES DE SECURITE

Le produit ACIDCryptofiler fourni par le commandement des réseaux particuliers de l'armement (CRPA) est la propriété du ministère des Armées. A ce titre, il est interdit de l'analyser, modifier ou de le détourner de sa finalité. **Il est également interdit d'en faire un usage privé, de le transmettre et de l'exploiter, sous quelle que forme que ce soit, hors du périmètre contractuel ou conventionnel dans lequel il a été fourni.**

8.1 HOMOLOGATION

Il ne peut être installé que sur des postes aptes à traiter les informations sensibles qu'il sert à protéger. Il ne doit pas être installé sur les postes de travail non administrés ou administrés à titre privé ou directement connectés à un réseau public de type internet sauf si celui-ci dispose de moyens de protection autorisés par le MinArm (notamment de filtrage) et homologué au niveau restreint.

La démarche d'homologation est un préalable à toute mise en service d'un système d'information quel que soit son niveau de sensibilité ou de classification. Elle consiste à évaluer les risques encourus afin de les traiter ou de les accepter. Elle fournit un niveau de confiance dans l'usage et la protection des informations et du système d'information.

8.2 NOMADISME

L'usage du logiciel ACID Cryptofiler est autorisé sur les postes de travail nomades (ou supports amovibles)

- protégés par un chiffrement de surface qualifié au niveau des informations à protéger ou
- non protégés par un chiffrement de surface qualifié au niveau des informations à protéger, sous réserve que la clé privée ACID soit stockée dans un volume chiffré de type ACID-Disk.

Après utilisation, l'utilisateur devra « démonter » le disque virtuel contenant sa clé. L'utilisateur ne doit pas avoir de copie de sa clé privée hors de l'ACID-Disk.

⁴ Des dérogations sont possibles dans le cadre d'accords de sécurité concernant les utilisateurs de nationalité hors UE et OTAN

En outre, le paramétrage relatif à la suppression des fichiers originaux doit être activé pour empêcher la présence conjointe d'un fichier en clair et chiffré sur le poste nomade.

En cas de transport, le support (poste de travail, clé USB, etc.) contenant la clé ACID doit rester en permanence sous la surveillance du détenteur.

8.3 LE CORRESPONDANT ACID

Pour obtenir le logiciel ACID Cryptofiler ou effectuer une demande de clé ACID auprès de la DGA, chaque entité par l'intermédiaire du représentant de la personne morale doit désigner un correspondant ACID⁵ et des suppléants.

Cette désignation est effectuée en même temps que la demande d'obtention du logiciel ACID. Il est l'interlocuteur privilégié de la DGA pour tous les sujets ACID.

Il procède à la gestion des éléments secrets et des certificats locaux au profit des utilisateurs.

A ce titre, le correspondant ACID :

- effectue les demandes de clés vers la DGA et en assure la cohérence et la qualité ;
- organise la distribution des clés au sein de son entité via la chaîne fonctionnelle SSI ;
- met en place les processus de révocation, suppression des bénéficiaires de clés ACID de son entité ;
- veille au respect des règles de sécurité de la présente instruction.

Le fichier de clés privées d'une part, et le mot de passe de protection d'autre part, doivent être transmis par des moyens distincts, aptes à protéger des données sensibles de niveau DR. Il est recommandé de remettre ces éléments à leurs utilisateurs en main propre ou par un moyen garantissant l'identité de leur destinataire. Les mots de passe ne doivent pas être envoyés en clair sur un réseau informatique.

En aucun cas, le correspondant ACID ne procède à une sauvegarde des clés ACID et des mots de passe en clair sur le réseau.

La désignation d'un correspondant ACID est obligatoire. En cas de cessation de fonction, un autre correspondant devra être désigné par le représentant de la personne morale.

9. OBTENTION DU LOGICIEL ACID CRYPTOFLER

9.1 ACCES A LA BIBLIOTHEQUE FR

La mise à disposition du logiciel ACID Cryptofiler et de ses bibliothèques cryptographiques nécessite la rédaction d'une « fiche justificative du besoin »⁶ dans laquelle le correspondant du MinArm définit le contexte d'emploi de la solution ACID.

Les demandes d'obtention du logiciel ACID Cryptofiler seront adressées au CRPA à l'adresse fonctionnelle (dga-ssdi-acid-industriel.contact.fct@intradef.gouv.fr) accompagnées :

- de la fiche justificative du besoin ;
- de la désignation du correspondant ACID ;

⁵ Officier de sécurité des systèmes d'information, Correspondant SSI, Officier chiffre
Formulaire SDI SecNum n°2332 ACID Engagement Correspondant, insérés au sein du Kit SDI SecNum ACID Personne morale

⁶ Formulaire SDI SecNum n°2330 ACID Fiche justificative, inséré au sein du Kit SDI SecNum ACID personne morale

- des engagements de responsabilité⁷.

L'objet du courriel devra être formaté de la façon suivante :

« Logiciel ACID [FR] [nom entité]⁸ [date]⁹ »

Toute demande non conforme sera automatiquement rejetée.

9.2 ACCES AUX BIBLIOTHEQUES UE ET OTAN

La demande d'obtention du logiciel contenant les bibliothèques UE ou OTAN sera effectuée par l'intermédiaire d'un point de contact (POC) DGA. Pour rappel, ces bibliothèques ont vocation à n'être utilisées que dans le cadre d'échanges avec des partenaires étrangers.

Les demandes d'obtention du logiciel ACID Cryptofiler seront adressées au CRPA à l'adresse fonctionnelle (dga-ssdi-acid-industriel.contact.fct@intradef.gouv.fr), accompagnées :

- la désignation d'un correspondant ACID au sein de l'entité bénéficiaire ;
- la fiche justificative du besoin ;
- la liste des utilisateurs de clés à doter au format Excel¹⁰ ;
- l'autorisation du Bureau de la sécurité des affaires internationales (BSAI) dga-ssdi.ai.fct@intradef.gouv.fr

L'objet de l'email devra être formaté de la façon suivante :

« Logiciel ACID [(UE) ou (OTAN)] [nom entité]¹¹ [date]¹² »

Le POC DGA assurera le rôle de correspondant ACID vis-à-vis du CRPA et assurera l'interface avec les correspondants ACID des entités de son périmètre.

10. OBTENTION DES CLES ACID

La production de clés ACID assurée par le CRPA est au profit des personnels appartenant à des EPA (établissement public administratif) et EPIC (établissement public industriel et commercial) sous tutelle de la DGA ou aux entités de droit privé dans le cadre des opérations d'armement, des projets et des marchés de la DGA, ayant besoin d'échanger avec le MinArm dans la limite du contexte d'emploi défini dans la fiche justificative du besoin.

Dans le cadre des marchés de la DGA, les plans contractuels de sécurité (PCS) doivent indiquer la mise en œuvre de la solution ACID et les systèmes d'information envisagés pour le déploiement du logiciel ACID Cryptofiler.

L'objet du courriel devra être formaté de la façon suivante :

« Clés ACID [FR] [nom entité]¹³ [date]¹⁴ »

La production de clés FR étant mensuelle, tous les besoins seront inscrits dans un unique tableau Excel¹⁵, chiffré dans un conteneur ACID, et transmis par courriel adressé au CRPA (et

⁷ Formulaires SDI SecNum n°2331 ACID Engagement personne morale et SDI SecNum n°2332 ACID Engagement Correspondant, insérés au sein du Kit SDI SecNum ACID Personne morale

⁸ Choisir un nom et s'y maintenir dans le temps

⁹ Mettre la date sous la forme : JJ-MM-AAAA

¹⁰ Modèle SDI SecNum n°2333 Demande de clef ACID, inséré au sein du Kit SDI SecNum ACID Personne morale

¹¹ Choisir un nom et s'y maintenir dans le temps

¹² Mettre la date sous la forme : JJ-MM-AAAA

¹³ Même nom que pour demande du logiciel

¹⁴ Mettre la date sous la forme : JJ-MM-AAAA

¹⁵ Modèle SDI SecNum n°2333 Demande de clef ACID, inséré au sein du Kit SDI SecNum ACID Personne morale

au maximum une (1) fois par mois). Dans le cas contraire, leur prise en compte et leur traitement n'est pas garanti.

Le CRPA transmettra les clés au correspondant ACID dans un conteneur chiffré avec ACID. Cette fourniture sera réalisée en deux étapes : un premier courriel (conteneur avec les clés publiques et les mots de passe), suivi d'un second (conteneur avec les clés privées) dès que le CRPA aura reçu l'accusé de réception du premier courriel.

Les correspondants ACID devront s'assurer que les procédures d'exploitation et de sécurité (PES) des systèmes d'information hébergeant ACID prévoient la signature d'une reconnaissance de responsabilité par les utilisateurs du logiciel et des clés ACID.

Les demandes de clés ACID devront être effectuée auprès du CRPA à l'adresse fonctionnelle : dga-ssdi-acid-industriel.contact.fct@intradef.gouv.fr

Les clés ACID privées sont à usage strictement personnel.

La cession ainsi que le prêt d'une clé ACID sont interdits.

Dans le cas de clés UE et OTAN, les demandes seront effectuées par le POC DGA désigné et validées par le BSAI ¹⁶ (dga-ssdi.ai.fct@intradef.gouv.fr).

L'objet du courriel devra être formaté de la façon suivante :

« Clés ACID [(UE) ou (OTAN)] [nom entité]¹⁷ [date] »

Le POC DGA aura aussi pour mission de distribuer les clés à ses correspondants ACID désignés au sein des entités privées ou étatiques pour lesquelles le besoin est exprimé.

11. RENOUVELLEMENT DES CLES

Chaque année de janvier à avril un renouvellement des clés arrivant à péremption a lieu.

Tous les correspondants ACID des entités concernées recevront un courriel listant les clés arrivant à échéance.

Si le renouvellement est nécessaire, les documents suivants devront être joints en retour du courriel de sollicitation :

- fiche justificative du besoin à jour¹⁸ ;
- le tableau Excel des clés¹⁹ à renouveler.

12. CESSATION DE FONCTION D'UN COLLABORATEUR

Tout collaborateur cessant les activités justifiant le besoin d'ACID devra :

1. s'assurer qu'il ne laisse aucun document chiffré inexploitable car non déchiffrable ;
2. détruire tous les exemplaires de sa clé privée et mots de passe correspondants avec la fonction d'effacement sécurisé du logiciel ACID Cryptofiler ;
3. désinstaller ou faire désinstaller le logiciel ACID Cryptofiler de tous ses postes de travail.

¹⁶ Bureau de la sécurité des affaires internationales

¹⁷ Même nom que pour demande du logiciel

¹⁸ Formulaire SDI SecNum n°2330 ACID Fiche justificative, inséré au sein du Kit ACID Personne morale

¹⁹ Modèle SDI SecNum n°2333 Demande clef ACID

13. COMPROMISSION D'UNE CLE PRIVEE OU DU MOT DE PASSE

En cas de compromission d'une clé privée ou de son mot de passe, il est impératif d'identifier, d'isoler et de protéger rapidement les conteneurs ACID susceptibles d'être compromis au niveau du détenteur lui-même et de ses correspondants.

En cas de perte, vol, incident de sécurité concernant une clé privée, le détenteur doit alerter sans délai son OSSI et son correspondant ACID qui remontera un compte-rendu d'incident (CRI) dans un conteneur ACID, à l'adresse fonctionnelle: dga-ssdi-acid-industriel.contact.fct@intradef.gouv.fr

Le CRI devra indiquer :

- le nom et prénom du détenteur de la clé compromise ;
- l'identification du périmètre d'emploi au profit duquel elle a été utilisée (FR, UE ou OTAN) ;
- la nature des informations compromises ;
- les actions immédiates prises pour circonscrire l'incident.

14. ENREGISTREMENTS

Enregistrements	Identification	Stockage	Protection (dégradation)	Accessibilité	Durée de conservation (Durée d'utilité administrative (DUA))	Élimination (sort final)
Fiches justificatives du besoin de dotation du logiciel et des clés ACID CRYPTOFLER et pièces justificatives	Le document sera enregistré dans un dossier portant le nom de la personne morale	Numérique (IsiFISH, dossier du CRPA)	Non protégé	Sur demande auprès du CRPA	5 ans après le dernier renouvellement de l'entité	Suppression numérique
Engagements de responsabilité de la personne morale	Le document sera enregistré dans un dossier portant le nom de la personne morale	Numérique (IsiFISH, dossier du CRPA)	Non protégé	Sur demande auprès du CRPA	5 ans après le dernier renouvellement de l'entité	Suppression numérique
Engagements de responsabilité du correspondant ACID	Le document sera enregistré dans un dossier portant le nom de la personne morale	Numérique (IsiFISH, dossier du CRPA)	Non protégé	Sur demande auprès du CRPA	5 ans après le dernier renouvellement de l'entité	Suppression numérique
Tableaux Excel de demande de clés ACID	Le document sera enregistré dans un dossier portant le nom de la personne morale	Numérique (IsiFISH, dossier du CRPA)	Non protégé	Sur demande auprès du CRPA	5 ans après le dernier renouvellement de l'entité	Suppression numérique

Les règles d'archivage du séquestre des clés ACID ne figure pas dans la présente procédure en raison de son niveau de protection.