Fiche Pratique N°68 : Chiffrez vos SMS avec foomms et foodjis V1.0

10 nov, 2026 · @Gabriel

Objectif : *signer et chiffrer vos SMS et MMS avec une identité OpenPGP gardée sur une clé de sécurité physique, sans compte ni serveur, grâce à foodjis et foomms, deux applications libres de l'association foopgp (Friends of OpenPGP).*

- ***Public visé :*** *intermédiaire (débutant accompagné)*
- ***Temps estimé :*** *1 heure une fois (identité et clé), puis 2 minutes par contact*
- ***Difficulté :*** *★★★☆☆ (Moyen)*
- ***Concerne :*** *Android uniquement (foomms : Android 8 ou plus, foodjis : Android 7 ou plus), avec lecteur NFC*
- ***Prérequis :*** *une clé de sécurité OpenPGP sans contact (NFC), une imprimante, et au moins un correspondant prêt à faire la même démarche*
- ***Fiches associées :*** *N°15 (messageries sans numéro), N°18 (double authentification), N°37 (vérifier une signature GPG), N°47 (arnaques en ligne), N°52 (confidentialité du téléphone), N°64 (téléphone sans Google)*

PARTIE 1 : LES BASES (pour débutants)

1. Le problème : le SMS est une carte postale

Un SMS ou un MMS voyage en clair. L'opérateur peut le lire et le conserver, et rien ne garantit qui l'a vraiment envoyé : n'importe qui peut afficher un faux nom d'expéditeur.

Situation	Conséquence
Un SMS passe par le réseau de l'opérateur	Son contenu est lisible, comme une carte postale
Un escroc envoie un SMS au nom de votre banque ou d'un proche	Rien ne prouve que le message vient vraiment de lui
Vous envoyez une photo de document par MMS	Elle circule et reste stockée sans protection
Les messageries chiffrées passent par Internet	Il faut des données mobiles, un compte et souvent un serveur

Une image pour comprendre : foomms glisse votre carte postale dans une enveloppe scellée. Le sceau (la signature) prouve que c'est vous. L'enveloppe (le chiffrement) ne s'ouvre qu'avec la clé physique du destinataire, qu'il garde dans sa poche.

Le risque : des messages lus par d'autres, et de faux messages crédibles à votre nom ou à celui de vos proches.

Le bénéfice : des SMS signés et chiffrés, sans Internet, sans compte et sans serveur intermédiaire. La clé privée ne quitte jamais votre clé de sécurité.

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°68 : Chiffrez vos SMS avec foomms et foodjis V1.0

2. Comprendre les outils

Élément	Rôle	L'image
Clé de sécurité (YubiKey 5 NFC, Nitrokey 3A…)	Garde vos clés privées, qui n'en sortent jamais	Le sceau et la clé du coffre, dans votre poche
PGP ID	Votre identité numérique, calculée à partir d'un lieu et d'un instant de naissance	Votre carte d'identité numérique
foodjis	Crée l'identité, l'écrit sur la clé, gère vos contacts, chiffre et vérifie	Le notaire de la maison
foomms	Messagerie SMS et MMS qui confie toute la cryptographie à foodjis	Le facteur qui met les lettres sous enveloppe
Fragments QR imprimés	Sauvegarde de vos secrets sur papier : par défaut, 3 fragments sur 5 suffisent	Le double des clés, confié à plusieurs proches

💡 foomms ne demande **pas l'accès à Internet** : les messages passent par le réseau de l'opérateur, sans serveur de l'association. Les deux applications sont libres (licence GPL 3), sans compte ni publicité.

3. Avant de commencer

- ☐ Mon téléphone est un Android 8 ou plus récent, avec **NFC** (Paramètres › tapez « NFC » dans la loupe)
- ☐ J'ai une clé de sécurité OpenPGP **sans contact** (voir section 4)
- ☐ J'ai une imprimante, et je sais où ranger les fragments imprimés
- ☐ J'ai une heure au calme pour la création de l'identité
- ☐ J'ai sauvegardé mes SMS actuels, par exemple avec **SMS Backup & Restore**
- ☐ Au moins un proche est prêt à faire la même démarche pour échanger des messages chiffrés

4. Obtenir une clé de sécurité

Option	Comment	À savoir
Par l'association foopgp	Souscrire sur HelloAsso, en donnant l'adresse e-mail de votre future identité	La clé est fournie aux membres dès que leurs souscriptions cumulées atteignent 6,42 Ɉ (environ 170 € en novembre 2026) ; le seuil évolue chaque mois
En l'achetant vous-même	Chez Nitrokey (fabricant allemand, matériel libre) ou Yubico	Choisissez un modèle **OpenPGP avec NFC**

⚠️ L'association **ne vend pas** ses clés : elle les fournit à ses membres, au choix et selon le stock (YubiKey 5 NFC, Nitrokey 3A, YubiKey 5C NFC).

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°68 : Chiffrez vos SMS avec foomms et foodjis V1.0

5. Installer foodjis et créer votre identité

1. Installez **foodjis** depuis Google Play, ou téléchargez le fichier APK sur `foodjis.foopgp.org`, avec son empreinte et sa signature.
    - Vous devez voir : l'application foodjis dans la liste de vos applications.
2. Ouvrez foodjis et choisissez de **créer une identité**. Placez le point sur la carte (ou utilisez **Here**), puis saisissez l'instant de naissance en heure locale.
    - Vous devez voir : un identifiant qui commence par `u4` (la variante réservée aux personnes).
3. **Imprimez les fragments QR** de sauvegarde. Rangez-les dans des lieux différents, ou confiez-en à des proches.
    - Vous devez voir : plusieurs feuilles de QR codes ; par défaut, 3 fragments sur 5 suffisent pour reconstituer l'identité.
4. **Configurez la clé** : tenez-la contre le dos du téléphone. Une clé neuve peut demander d'abord trois secondes d'alimentation sur un port USB, par exemple un chargeur.
    - Vous devez voir : le **PIN** et le **code Admin**, affichés une seule fois. Notez-les sur papier.
5. Complétez votre carte (nom d'usage, adresses) : chaque changement est signé par la clé, puis publié sur les serveurs de clés.
    - Vous devez voir : votre carte à jour dans foodjis.

⚠️ Le PIN et le code Admin ne s'affichent qu'une fois, et l'écran est protégé contre les captures. Rangez-les avec les fragments imprimés.

6. Installer foomms et envoyer vos premiers messages

1. Installez **foomms** depuis Google Play, ou par le fichier APK sur `foomms.foopgp.org`. Avec l'APK, Android peut exiger d'autoriser les **paramètres restreints** : dans les paramètres de l'application, menu ⋮ en haut à droite.
    - Vous devez voir : foomms dans vos applications.
2. Faites de foomms votre **application SMS par défaut**.
    - Vous devez voir : vos conversations dans foomms.
3. Associez chaque contact à **son certificat**, avec son accord : échange en face à face par QR code, par fichier, ou depuis les serveurs de clés.
    - Vous devez voir : le certificat enregistré dans le carnet d'adresses du contact.
4. Écrivez un message : il est signé et chiffré selon vos réglages. Un texte court part en SMS ; un texte long part en un seul MMS.
    - Vous devez voir : une bulle de couleur (voir section 7).
5. Pour lire un message chiffré, appuyez dessus et présentez la clé au dos du téléphone.
    - Vous devez voir : le texte en clair, gardé en mémoire 5 minutes par défaut, et jamais écrit sur le téléphone. Un seul appui ouvre aussi les messages voisins (7 de chaque côté par défaut).

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°68 : Chiffrez vos SMS avec foomms et foodjis V1.0

7. Lire les couleurs

Couleur	Signification
Vert	Chiffré et certifié : la protection complète
Bleu	Certifié seulement : on sait qui l'a écrit
Jaune	Chiffré seulement
Rouge	Ni chiffré ni certifié : un SMS ordinaire
Gris	Message chiffré pas encore ouvert

8. À quoi s'attendre, et que faire si...

Symptôme	Cause possible	Action
La clé n'est pas détectée	NFC désactivé, ou clé mal placée	Activez le NFC, déplacez lentement la clé au dos du téléphone, retirez une coque épaisse ou métallique
Une clé neuve ne répond pas	Elle a besoin d'être alimentée une première fois	Branchez-la trois secondes sur un chargeur USB, puis recommencez
Le message part en rouge	Le contact n'a pas de certificat associé	Associez son certificat (section 6, étape 3)
Votre correspondant reçoit un texte illisible	Il n'a pas foomms	Il peut copier le texte dans foodjis pour le déchiffrer
Vous ne relisez plus vos messages envoyés	L'option « chiffrer aussi pour soi » est désactivée	Activez-la dans les réglages de foomms
La photo envoyée est moins nette	Un MMS reste sous 300 Ko : la photo est réduite avant chiffrement	C'est normal ; envoyez l'original autrement si besoin
Un MMS de groupe arrive abîmé	Certains opérateurs réécrivent les destinataires ou retirent des pièces jointes	Mettez à jour foomms (correctifs annoncés en version 1.4.1)
La clé refuse le PIN	Trop d'essais faux : la clé se bloque	Utilisez le code Admin noté à la création
Vous avez perdu la clé	L'identité n'est plus utilisable avec elle	Reconstituez l'identité sur une nouvelle clé avec les fragments imprimés

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°68 : Chiffrez vos SMS avec foomms et foodjis V1.0

PARTIE 2 : ALLER PLUS LOIN (pour intermédiaires et avancés)

9. foomms ou une messagerie par Internet ?

Outil	Réseau	Compte	Les clés privées	Plateformes
foomms	Réseau téléphonique (SMS, MMS), sans Internet	Aucun	Sur votre clé physique	Android
Element (fiche N°33)	Internet, serveurs Matrix décentralisés	Un identifiant, sans numéro obligatoire	Dans l'application	Android, iPhone, ordinateur
SimpleX (fiche N°15)	Internet, relais sans identifiant	Aucun	Dans l'application	Android, iPhone, ordinateur
Signal	Internet, serveurs de Signal	Numéro de téléphone	Dans l'application	Android, iPhone, ordinateur

💡 foomms est précieux là où Internet manque, ou quand on veut **prouver** l'expéditeur d'un SMS. Pour les conversations de groupe et les appels, une messagerie par Internet reste plus pratique.

10. Cas avancés

Courriel chiffré : foodjis se propose comme fournisseur OpenPGP du système. Thunderbird pour Android peut alors signer, chiffrer, ouvrir et vérifier vos courriels avec la même clé.

SSH et git : foodjis peut servir d'agent SSH : la même clé de sécurité ouvre vos connexions SSH et signe vos commits git, une demande à la fois.

Sur ordinateur : Djibian, la configuration GNU/Linux de l'association, propose les mêmes parcours que foodjis. L'association organise des ateliers Djibian et OpenPGP.

Vérifier le téléchargement : chaque fichier APK est publié avec son empreinte SHA-256 et une signature PGP détachée. Sur un ordinateur Linux (voir la fiche N°37) :

```
sha256sum foomms_1.4.1.apk
cat foomms_1.4.1.apk.sha256
gpg --verify foomms_1.4.1.apk.asc foomms_1.4.1.apk
```

Les deux empreintes doivent être identiques. La vérification de la signature suppose d'avoir le certificat public de l'auteur.

Sauvegarder ses SMS : foomms utilise le format lu par SMS Backup & Restore ; les messages chiffrés restent chiffrés dans la sauvegarde.

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°68 : Chiffrez vos SMS avec foomms et foodjis V1.0

11. À savoir avant de se lancer

Crainte fréquente	La réalité
« Si je perds la clé, je perds tout. »	Les fragments imprimés permettent de reconstituer l'identité : par défaut, 3 sur 5 suffisent.
« Tous mes correspondants doivent l'avoir. »	La signature fonctionne avec tout le monde. Le chiffrement suppose que le destinataire ait un certificat ; sans foomms, il peut déchiffrer en collant le texte dans foodjis.
« L'association peut lire mes messages. »	Il n'y a pas de serveur : foomms n'a même pas l'accès à Internet, et la clé privée ne quitte jamais votre clé.
« Mon opérateur ne voit plus rien. »	Il ne lit plus le contenu, mais il voit toujours qui écrit à qui, et quand.
« C'est trop compliqué. »	Une heure, une fois. Ensuite, il suffit de poser la clé contre le téléphone.
« Il faut passer par Google Play. »	Non : les fichiers APK signés sont proposés sur les sites officiels.
« Ça marche aussi sur iPhone. »	Non : foodjis et foomms existent uniquement sur Android.

12. Challenge 7 jours

- **Jour 1 :** créer votre identité dans foodjis et imprimer les fragments.
- **Jour 2 :** ranger les fragments dans au moins trois lieux différents.
- **Jour 3 :** installer foomms et envoyer un premier SMS signé à un proche.
- **Jour 4 :** échanger vos certificats en face à face, par QR code.
- **Jour 5 :** envoyer votre premier SMS chiffré.
- **Jour 6 :** régler la durée d'ouverture des messages et tester la lecture avec la clé.
- **Jour 7 :** montrer la démarche à un proche.

Vous allez constater : un SMS vert rassure. Vous savez qui vous écrit, et personne d'autre ne peut lire.

13. En résumé (ce que vous gagnez)

Action	Gagné	Renvoi
Créer une identité PGP ID sur une clé	Une identité que personne ne peut vous prendre	Section 5
Imprimer les fragments QR	Rien n'est perdu si la clé l'est	Section 5
Faire de foomms votre messagerie	Des SMS signés et chiffrés, sans Internet	Section 6
Certifier vos contacts	Plus de faux messages à leur nom	Section 6

gabriel.ananda@mailo.com
CC BY SA

Fiche Pratique N°68 : Chiffrez vos SMS avec foomms et foodjis V1.0

Action	Gagné	Renvoi
Utiliser la même clé pour le courriel et SSH	Une seule clé pour tout signer	Section 10

14. À retenir absolument

- La clé privée reste **sur votre clé de sécurité** : le téléphone ne la voit jamais.
- **Imprimez et rangez les fragments** : c'est votre double des clés.
- Le PIN et le code Admin ne s'affichent **qu'une fois** : notez-les.
- L'opérateur ne lit plus vos messages, mais il voit **qui écrit à qui**.

Test final :

1. Mon téléphone a le NFC et foodjis reconnaît ma clé.
2. Mes fragments sont imprimés et rangés en lieu sûr.
3. foomms est ma messagerie par défaut.
4. J'ai envoyé un message vert à un proche. ✅

Références

- foopgp – Friends of OpenPGP, page d'accueil de l'association
- foopgp – foomms : SMS et MMS dans une enveloppe PGP (article du 6 novembre 2026)
- foopgp – foodjis est disponible sur Android (article du 24 septembre 2026)
- foopgp – Usage avancé : foodjis comme agent SSH pour Android
- foomms – site officiel (prérequis, téléchargement, licence)
- foodjis – site officiel (prérequis, téléchargement, licence)
- foodjis – clés de sécurité fournies aux membres
- foopgp – PGP ID, une identité numérique ancrée dans une clé physique
- foopgp – Retour d'expérience, rapport de stage (juin 2024)
- Google Play – foomms
- Google Play – foodjis
- Codeberg – organisation foopgp

gabriel.ananda@mailo.com
CC BY SA