

Expiration de certificats IngeTrust

Questions fréquentes

Mise à jour 04 Décembre 2019

www.ingenico.com

28/32, boulevard de Grenelle, 75015 Paris - France / (T) +33 (0)1 58 01 80 00 / (F) +33 (0)1 58 01 91 35

Ingenico France– SAS au capital de 18 500 € / 538 600 404 RCS PARIS

Qu'est-ce qu'IngeTrust ?

Mise en place en 2009, IngeTrust est l'infrastructure à clé publique d'Ingenico, qui utilise des certificats pour les terminaux Telium.

Pourquoi les certificats expirent-ils ?

Les certificats servent à la sécurisation des données. PCI impose une durée de vie limitée. Habituellement 10 ans de durée de vie sont appliqués.

Quand les certificats IngeTrust expirent-ils ?

Les certificats expirent au bout de 10 ans, certains terminaux expireront le 14 Avril 2021 ou le 29 Décembre 2021.

Concrètement quels sont les terminaux concernés ?

Les terminaux concernés sont : iCT220, iCT250, iWL250, iWL280, iSMP, iCMP, iPP220, iPP280, iPP310, iPP320, iPP350, iHC950, Gamme ISelf.

Les terminaux Tetra sont-ils impactés par la fin de vie des certificats ?

Les certificats des terminaux Tetra expirent à date de fabrication +10 ans, ils ne sont pas concernés par l'échéance de 2021.

Quelle est la fin de vie PCI théorique des terminaux ?

Le GIE Carte Bancaire par son programme REMPARTS demande la fin de vie des terminaux PCI v2 le 31 Décembre 2020 et des terminaux PCI v3 le 31 Décembre 2023 (Plus un an pour les automates).

Est-ce que la configuration logicielle influence la perte de certificat ?

Non, toutes les configurations logicielles sont concernées.

Quelle est la conséquence de l'expiration des certificats IngeTrust?

La conséquence est double :

- Perte de la communication entre le terminal et un PinPad.
- Impossibilité de réaliser une connexion sécurisée (principalement pour le téléchargement des clés).

Les conséquences sont identiques pour la gamme ISelf entre l'IUP et ses périphériques.

Quelle est la conséquence de la perte de communication entre le terminal et le PinPad ?

Si le terminal est PCI v2 connecté à un iPP2, la communication reste valide tant que ni le terminal, ni le PinPad ne sont remplacés.

Si le terminal est PCI v3 ou PCI v2 connecté à un iPP310, le PinPad devient non fonctionnel et n'est plus reconnu par le terminal, dans une latence de 8 heures après expiration du certificat si un reboot est effectué (cf. annexe 1). Le terminal continue à fonctionner seul mais sa configuration doit être modifiée dans les menus de paramétrage afin de ne plus utiliser de PinPad.

Dans le cas d'un ISelf PCI v3, les périphériques deviennent non fonctionnels et ne sont plus reconnus par l'IUP dans une latence de 8 heures après expiration du certificat (cf. annexe 2).

Que se passe-t-il dans le cas où seul le certificat du terminal ou du PinPad est échu ?

Si le PinPad seul est échu :

- Il est possible de remplacer le PinPad. La communication sera à nouveau fonctionnelle.

Si le Terminal seul est échu :

- Il est possible de remplacer le Terminal. La communication sera à nouveau fonctionnelle.

Quel est le message affiché sur le terminal lorsque la communication PinPad devient non fonctionnelle ?

Le message affiché sur l'iCT après expiration du certificat est « PINPAD HORS SERVICE ».

Le message affiché sur l'iSELF après expiration du certificat est « IUR250 ERREUR »

Quelle est la conséquence de l'impossibilité de réaliser un téléchargement sécurisé ?

Il devient impossible de réaliser à distance une injection de clé, par exemple pour l'utilisation de PIN on-line nécessitée par la plupart des logiciels UPI (Union Pay International).

Il devient impossible de réaliser une connexion sécurisée, par exemple pour l'utilisation d'une authentification forte avec un système tiers.

La connexion à Axis est-elle impactée ?

Un terminal dont les certificats ont expiré ne peut plus se connecter à Axis.

Tous les terminaux sont-ils concernés ?

Non, les terminaux fabriqués après mi 2016 ou passés en centre de réparation depuis Décembre 2016 ne sont pas concernés car leurs certificats ont été mis à jour. Les terminaux Tetra ne sont pas impactés.

Certains certificats ont-ils expiré en 2019 ?

Oui les certificats de certains terminaux ont expiré le 14 Mai et le 9 Juin 2019. Etant PCI v2 le chargement sécurisé n'est plus possible mais la communication entre ces terminaux et leur Pin Pad reste valide. Cependant il n'est pas possible de connecter un nouveau PinPad sur ces produits.

Est-il possible de connaître la date d'expiration des certificats de mon terminal ?

Non, il n'est pas possible de connaître la date de fin de vie des certificats de son terminal depuis l'écran du terminal.

Peut-on étendre la durée de vie des certificats ?

Oui, pour tous les terminaux il est possible d'étendre la durée de vie des certificats IngeTrust, par réactivation en centre de réparation.

Pour les terminaux qui ont une échéance au 14/04/2021 ou 29/12/2021 il est également possible d'étendre la durée de vie des certificats par chargement local ou téléchargement d'une application IKR dédiée.

Qu'est-ce que l'application IKR ?

L'application IKR, Ingetrust Key Renewal, est une application à charger sur le terminal et qui va mettre à jour les certificats sur le terminal. Elle nécessite une connexion vers un serveur Ingenico.

Quelle est la taille de l'application IKR ?

L'application IKR qui permet la mise à jour des certificats nécessite 250K de mémoire flash disponible dans le terminal.

Est-ce qu'il est possible de faire la mise à jour par RTC ?

La mise à jour est possible en RTC, ou en IP (GPRS, 3G ou ETH)

Quelle est la durée de la mise à jour ?

L'application IKR nécessite environ 5 minutes de temps de traitement à l'issue duquel un ticket est imprimé, précisant la bonne génération des clés. Durant la procédure de mise à jour, le terminal n'est pas utilisable. Cependant, il est possible d'interrompre la procédure et de relancer plus tard l'application.

Comment l'application IKR est-elle disponible ?

L'application IKR peut être injectée dans le terminal par téléchargement sur notre serveur TEM ou par chargement local.

Le téléchargement peut être déclenché manuellement, par réception d'une Enveloppe du serveur bancaire ou par un appel via l'application TMSCall ou TConnect.

L'application IKR reste-elle efficace après que le certificat IngeTrust ait expiré ?

Non, si le certificat a expiré, la mise à jour à distance des clés IngeTrust par l'application IKR n'est plus possible.

Le Pin Pad est-il mis à jour si je mets à jour le terminal ?

Oui, si je mets à jour mon terminal avec l'application IKR, le Pin Pad connecté au terminal est également mis à jour. Lors de la mise à jour de l'IUP2x alors ses périphériques sont aussi mis à jour.

Comment puis-je savoir si mes produits sont impactés ?

Ingenico fournit les numéros de série des terminaux impactés.

Comment puis-je savoir si mes produits ont été mis à jour ?

Ingenico fournira régulièrement les numéros de série des terminaux mis à jour.

Quelle est la durée de vie des certificats des terminaux 'étendus' ?

Les certificats chargés par l'application IKR sont étendus pour une durée de vie de 10 ans. De même les certificats des terminaux produits expirent 10 ans après leur date de fabrication.

ANNEXE 1 : Tableau de compatibilité Terminaux

	iPP220 PCI v2	iPP280 PCI v2	iPP310 PCI v2	iPP280 PCI v3	iPP310 PCI v3
ICT2xx PCI v2	Maintien de la communication entre le TPE et le PP après l'expiration des certificats Perte de la connexion distante sécurisée		Perte de la communication entre le TPE et le PP ainsi que de la connexion distante sécurisée après un reboot avec une latence possible de 8h après l'expiration	Configuration non disponible	
ICT2xx PCI v3	Configuration non disponible			Perte de la communication entre le TPE et le PP ainsi que de la connexion distante sécurisée après un reboot avec une latence possible de 8h après l'expiration	
IWL2xx PCI v2 PCI v3	Perte de la connexion distante sécurisée				

ANNEXE 2 : Tableau de compatibilité AUTOMATES

	iUR250 PCI v3	iUC150 + iUR250 PCI v3	iUC150B + iUR250 PCI v3
IUP2xx PCI v3	Perte de la communication entre l'IUP2xx et ses périphériques ainsi que de la connexion distante sécurisée automatiquement dans les 8h suivant l'expiration		

iUC180B PCI v3	Perte de la connexion distante sécurisée
-------------------	--