

**Targeted Long Term Financing Operation (TLTRO)**

Modalités techniques de communication du reporting statistique entre les établissements de crédit et la Banque de France

Le reporting statistique ainsi que toute information afférente prévue dans le cadre du TLTRO devront être transmis au Service des Statistiques Européennes de la Banque de France par **courriel** à l’adresse suivante :

[**1417-tltro-ut@banque-france.fr**](mailto:1417-tltro-ut@banque-france.fr)**.**

Dans la mesure où les données demandées par la Banque de France revêtent un caractère **confidentiel**, la Banque de France demande de « **chiffrer » (autrement dit crypter)[[1]](#footnote-1)** les échanges de courriels effectués au titre du reporting statistique. Un mécanisme de sécurité peut s’implémenter à divers niveaux dans le protocole d’échange par courriel. . La Banque de France propose deux options:

**Option A (à privilégier) :** utilisation d’une sécurisation *TLS* (*Transport Layer Security*, sécurité de la couche de transport, parfois connue sous le nom de SSL).

Il s’agit d’un protocole normalisé supporté par tous les équipements de messagerie à l’état de l’art, très simple d’utilisation puisque cela ne nécessite aucune action des utilisateurs. Cette sécurité technique et invisible doit être vérifiée ou mise en place par les services informatiques. La Banque de France a pu vérifier que les échanges de courriels avec plusieurs grands groupes bancaires sont d’ores et déjà protégés par cette technologie.

Les établissements qui opteront pour la sécurité technique *TLS* devront communiquer à la Banque de France les adresses de messagerie des interlocuteurs désignés dans le cadre du TLTRO, ainsi que les coordonnées d’un technicien informatique susceptible d’être contacté par la Banque de France afin de vérifier, régler ou activer cette sécurité.

**Option B:** si la sécurisation *TLS* ne peut être mise en œuvre pour des raisons techniques, ou bien si elle n’est pas jugée satisfaisante par l’établissement, la Banque de France est en mesure d’implémenter une sécurisation à la main de l’utilisateur en s’appuyant sur le format de message *S/MIME*, lui aussi implémenté par l’ensemble des systèmes de messagerie électronique du marché qui met en œuvre les algorithmes de cryptographie au moyen de certificats numériques au format normalisé *X509*[[2]](#footnote-2). Cette solution, classiquement intégrée au logiciel de messagerie, permet à l’utilisateur de visualiser et s’assurer de la bonne sécurisation des messages, mais nécessite certaines actions, notamment l’installation de certificats. Deux certificats sont en effet nécessaires : l’un fourni par la Banque de France permet de chiffrer les messages émis par l’établissement, l’autre doit être acquis par l’établissement[[3]](#footnote-3) et communiqué à la Banque de France qui l’utilisera pour chiffrer les messages transmis.

Les établissements qui opteront pour la sécurité *S/MIME* devront communiquer à la Banque de France les coordonnées des interlocuteurs désignés dans le cadre du TLTRO ainsi que d’un technicien informatique. La Banque de France se mettra en relation avec ces correspondants afin de synchroniser les actions requises pour l’implémentation du dispositif.

**En raison des délais de délivrance des certificats, l’option B ne pourra être mise en place que pour les établissements participants qui se seront déclarés avant le 12 aout 15h30. L’option A restera proposée au-delà de cette échéance.**

En cas d’impossibilité avérée pour implémenter l’un ou l’autre des dispositifs, ou en cas de défaillance de la solution choisie en cours d’utilisation, les établissements pourront, à titre dérogatoire et en accord avec le Service des Statistiques Européennes, décider d’échanger par courriel non chiffré.

Pour toute question relative à la sécurisation des échanges de données entre les établissements et la Banque de France, les responsables à contacter à la Banque de France sont :

Roland Lubrano, chef du service des projets et des maintenances statistiques

e-mail : Roland.LUBRANODISCAMPAMORTE@banque-france.fr

Julien Dejean, adjoint au chef du service des projets et des maintenances statistiques

e-mail : julien.dejean@banque-france.fr

1. Dans le contexte de cette collecte, la Banque de France ne demande pas de « signer » les messages. [↑](#footnote-ref-1)
2. Un certificat numérique *X509* contient entre autres informations utiles :

   Une clé cryptographique dite « publique » ;

   L’identité du détenteur de la clé « privée » associée (tout ce qui est « verrouillé » avec une clé, ne peut-être « déverrouillé » qu’avec l’autre) ;

   La signature d’une autorité de certification garantissant les informations ci-dessus. [↑](#footnote-ref-2)
3. La Banque de France accepte les certificats répondant à un niveau de qualité minimal, notamment les certificats référencés par le Comité Français d’Organisation et de Normalisation Bancaire (« multi-acceptance »). La Banque de France peut également fabriquer et délivrer des certificats sur demande du mandataire de certificat de votre établissement. [↑](#footnote-ref-3)