

Déclaration des pratiques d'enregistrement (Délégation d'autorité d'enregistrement de l'IGC pilote du CRU)

1 Introduction

Supélec, campus de GIF sur Yvette, ci après noté SUPELEC-GIF souhaite qu'une partie de son personnel dispose de certificats électroniques.

Le CRU permet la délivrance des certificats émis par l'Autorité de Certification *ac-utilisateur* de son IGC pilote à ces populations, en déléguant la fonction d'Autorité d'Enregistrement (AE) à l'établissement pour l'enregistrement des demandes de certificats.

Du fait de la sensibilité de cette fonction, la délégation d'AE se fait sous des conditions précises détaillées dans le document intitulé *Convention de délégation d'Autorité d'Enregistrement de l'IGC pilote du CRU vers un établissement d'enseignement supérieur*, document qui doit être approuvé par le CRU, l'Université de Rennes 1 et SUPELEC-GIF.

SUPELEC-GIF s'engage entre autre à définir sa *Déclaration des Pratiques d'Enregistrement (DPE)*, objet du présent document, en détaillant les points suivants :

- population susceptible de demander un certificat,
- usage des certificats délivrés,
- procédure de validation des demandes et de révocations de certificats,
- disponibilité des services d'enregistrement de demande et de révocation.

2 Population susceptible de demander un certificat

Les certificats personnels émis par l'Autorité de Certification *ac-utilisateur* de l'IGC pilote du CRU pour SUPELEC-GIF, sont destinés aux personnels remplissant l'ensemble des conditions suivantes :

- personne physique (l'Autorité de Certification ne délivre pas de certificats de fonction), en activité, **enregistrée dans le référentiel des ressources humaines** de SUPELEC-GIF.
- ou autre membre du personnel autorisé au cas par cas par le Directeur Général de SUPELEC-GIF ou son représentant désigné.

Dans la suite du document, une personne remplissant les conditions énumérées ci-dessus sera appelée « personnel de SUPELEC-GIF ».

On rappelle que l'Autorité de Certification *ac-utilisateur* de l'IGC pilote du CRU n'émet **pas de certificats à destination des étudiants**.

Ces conditions sont applicables à la date de validation conjointe du présent document par le Service pilote d'IGC du CRU et par l'Autorité d'Enregistrement déléguée de SUPELEC-GIF; elles pourront être modifiées par la suite si nécessaire, mais devront, dans ce cas, faire l'objet d'une nouvelle validation des deux parties.

3 Usage des certificats délivrés

3.1 Sécurisation des accès et des flux réseau

Les certificats émis pourront être utilisés dans des mécanismes de **sécurisation d'applications ou de réseaux**. Ce volet comporte plusieurs points :

- l'utilisation des certificats pour **l'authentification de l'utilisateur**. L'identité ainsi vérifiée pourra servir de base à un contrôle d'accès aux ressources (accès à un réseau, à une application, à une fonction particulière d'une application, ...)
- **la sécurisation des flux réseau** en assurant leur **intégrité, l'authentification de l'origine** des messages, et leur **confidentialité**. Dans ce cadre les clés liées aux certificats interviennent dans la sécurisation des échanges de paramètres et de clés de sessions protégeant les flux

Le terme « sécurisation des flux réseau » comprend tous les mécanismes autorisés en France et permettant de **chiffrer l'information pendant sa transmission** (par exemple un VPN IPSec, une sécurisation de flux TLS/SSL). Ceci n'inclut pas les mécanismes servant à stocker l'information de manière chiffrée (à ce titre le chiffrement de courrier électronique est un cas à part, décrit dans le paragraphe 3.2.2).

3.2 Sécurisation de la messagerie

3.2.1 Assurer l'intégrité et l'authentification d'un message

Les certificats générés pourront aussi servir à leur propriétaire dans le cadre de la **messagerie électronique** afin :

- d'assurer l'authentification de l'émetteur d'un courrier électronique,
- d'assurer l'intégrité d'un courrier électronique (toute modification du courrier électronique entre son émission et sa réception est détectée),

Dans ce cadre, une signature numérique sera calculée sur le courrier électronique. Toutefois **cette signature n'a pas de valeur juridique**. En effet, conformément à la Politique de Certification (PC) de l'IGC pilote du CRU, les certificats émis :

- **ne pourront pas** être utilisés pour des applications de signature dans le cadre de la **dématérialisation d'actes**,
- **ne pourront pas** être utilisés pour des applications de sécurisation de **moyens de paiement ou d'applications financières**.

3.2.2 Assurer la confidentialité d'un message

Bien que techniquement possible et facile, l'usage des clés associées aux certificats pour du **chiffrement de courriers électroniques est soumis à conditions**.

En effet, une fois reçu, le message reste chiffré dans la boîte de réception du destinataire, or la justice peut en demander à tout moment la version en clair. Si l'utilisateur n'a plus en sa possession la clé privée (cas de perte ou de vol), il ne peut plus déchiffrer le message. **Ni l'IGC pilote du CRU, ni SUPELEC-GIF ne propose de service de recouvrement de clés**, ce qui signifie qu'une clé perdue par l'utilisateur ne peut être récupérée.

En conséquence, **l'usage du chiffrement est explicitement réglementé** :

- Son usage ne doit pas être systématique,
- Il est exclusivement réservé à de la correspondance confidentielle justifiant un chiffrement : transmission de mot de passe, diffusion de données financières confidentielles...

4 Procédures de gestion des certificats

4.1 La demande de certificat

La demande de certificat est réalisée par l'utilisateur. Cette phase permet notamment de vérifier que l'utilisateur a bien donné **une adresse de courrier électronique valide**.

L'utilisateur choisit de plus **un secret de validation** dont la connaissance sera nécessaire à l'opérateur d'enregistrement pour valider la demande de certificat.

Les modalités techniques de cette phase de demande de certificat peuvent être amenées à changer (l'interface est celle mise à disposition par le CRU) sans remettre en cause la présente DPE.

4.2 Procédure de validation des demandes de certificat

Une fois que la demande de certificat a été confirmée par le demandeur, un opérateur d'enregistrement (OE) de SUPELEC-GIF procède aux vérifications suivantes :

- Vérification de l'appartenance de la personne au référentiel du personnel de SUPELEC-GIF indiqué au chapitre 2
 - Si la date de fin d'appartenance de la personne au référentiel est connue, celle-ci est portée à la connaissance de l'opérateur d'enregistrement
- Vérification d'identité
 - Si l'utilisateur est présent (ou bien peut se déplacer) sur le campus, un rendez-vous de « visu » est planifié et le demandeur est informé qu'il devra présenter une pièce d'identité avec photo (carte nationale d'identité, passeport, carte d'identité professionnelle, permis de conduire)
 - Lors du rendez-vous l'identité est vérifiée : la photo de la pièce d'identité correspond à la personne qui se présente
 - Si le demandeur ne veut pas ou ne peut pas présenter une pièce d'identité avec photo et que le certificat demandé n'est pas indispensable à l'exécution d'une tâche professionnelle : l'opérateur peut refuser de valider la demande de certificat,
 - Si le demandeur ne veut pas ou ne peut pas présenter une pièce d'identité avec photo et que le certificat demandé est indispensable à l'exécution d'une tâche professionnelle : l'opérateur doit demander au Directeur Général de SUPELEC-GIF ou à son représentant désigné de certifier l'identité du demandeur
 - Une fois la vérification d'identité réalisée, le demandeur doit donner le secret de validation qu'il a choisi lors de la demande de certificat à l'opérateur
 - Si l'utilisateur n'est pas sur le campus de l'école et ne peut s'y rendre dans un délai raisonnable par rapport à son besoin de certificat, le rendez-vous se fera par téléphone uniquement au numéro donné par le service des ressources humaines

- La concordance entre le numéro de téléphone « officiel » de la personne et le secret de validation donné sert alors de preuve de l'identité du demandeur
- Cette procédure reste exceptionnelle et ne sera pas employée si un contact « de visu » est possible
- Validation du certificat
 - L'opérateur a donc vérifié l'identité du demandeur et connaît le secret de validation, il se connecte donc sur l'interface de l'autorité d'enregistrement légère (AEL) et valide la demande de certificat
 - La durée de validité du certificat est choisie en fonction du besoin de l'utilisateur et n'excède en aucun cas la durée maximale prévue par l'IGC pilote du CRU, ni la durée de son appartenance au référentiel de SUPELEC-GIF si celle-ci est prévisible.

4.3 Procédure de renouvellement d'un certificat

Dans les dernières semaines de la période de validité du certificat, le renouvellement du certificat peut être demandé.

La **demande de renouvellement** de certificat est **réalisée par l'utilisateur** sur l'interface de l'IGC pilote du CRU qui est prévenu par courrier électronique de l'approche de la date d'expiration de son certificat.

Conformément à la PC de l'IGC pilote du CRU, le renouvellement est soumis aux **mêmes vérifications qu'une demande initiale**. Toutefois la vérification d'**identité du demandeur est considérée comme acquise si** la demande de renouvellement est authentifiée par un **certificat encore valide émis par la même AC**.

Ainsi l'opérateur procédera comme indiqué au chapitre 4.2 pour valider la demande de renouvellement si le certificat a déjà expiré.

Si le certificat n'a pas expiré et que la demande est authentifiée, l'opérateur ne vérifiera pas l'identité du demandeur, mais contrôlera que **la personne appartient toujours au référentiel du personnel** de SUPELEC-GIF indiqué au chapitre 2.

Dans ce cas, le certificat peut être **renouvelé pour une période limitée** au minimum de la durée maximale prévue par l'IGC pilote du CRU et de la durée de son appartenance au référentiel de SUPELEC-GIF si celle-ci est prévisible.

4.4 Procédure de révocation des certificats

4.4.1 Causes de la révocation

Avant sa date limite d'utilisation, un certificat peut devenir inutilisable pour diverses raisons :

- le propriétaire du certificat **change de statut** (changement d'établissement, d'adresse électronique),
- le propriétaire du certificat **ne respecte pas les usages prévus pour les certificats** comme décrits dans la DPE de SUPELEC-GIF,

- le propriétaire du certificat **perd sa clé privée** (panne du disque dur, ...) ou bien oublie son mot de passe d'accès à cette clé
- une **compromission de la clé privée est soupçonnée** (utilisateur ayant laissé son poste de travail en accès libre sans avoir verrouillé par un mot de passe l'accès à sa clé privée)

Dans ces conditions, il est nécessaire de « **révoquer** » le certificat avant d'en générer éventuellement un nouveau. La révocation d'un certificat provoque la mise à jour d'une Liste de Révocation de Certificats (« CRL ») qui est disponible via une URL renseignée dans le certificat même de l'utilisateur (par exemple : <http://igc.cru.fr/cgi-bin/loadcrl?CA=ac-utilisateur&format=DER>). Cette liste peut être consultée à tout moment par les applications vérifiant les certificats (à condition que cette fonction soit disponible et activée).

La révocation d'un certificat doit se faire suffisamment rapidement pour limiter les risques d'utilisation frauduleuse du certificat, mais sans précipitation pour éviter que des demandes de révocation falsifiées ne provoquent un déni de service pour les utilisateurs.

4.5 Authentification de la demande de révocation

La révocation d'un certificat peut être demandé par :

- le propriétaire du certificat,
- l'opérateur d'enregistrement d'AEL,
- le RSSI de SUPELEC-GIF (Responsable de la Sécurité des Systèmes d'Information),
- le Directeur Général de SUPELEC-GIF ou son représentant désigné,
- le CRU, autorité administrative de cette IGC

La demande de révocation peut être réalisée par différents moyens :

- Un **rapport de « visu »** en présentant à l'opérateur d'enregistrement une pièce d'identité avec photographie dans le cas du propriétaire du certificat
- Par **mail signé**¹
- Par **Fax ou courrier traditionnel signé**

L'opérateur d'enregistrement pourra contacter l'utilisateur afin de savoir ce qui motive la révocation. Ceci doit permettre d'identifier des défauts dans les usages des certificats et de savoir si l'utilisateur a vraiment besoin d'un nouveau certificat.

5 Disponibilité des services d'enregistrement de demande et de révocation

5.1 Coordonnées

Le service de gestion de l'autorité d'enregistrement déléguée est assuré par les personnes de SUPELEC-GIF identifiées comme « opérateur d'enregistrement », « correspondant technique », « support utilisateur » pour l'IGC pilote du CRU et situées à l'adresse suivante :

¹ Nous acceptons la signature de cette demande avec la clé privée correspondant au certificat à révoquer. En effet, même s'il s'agit d'une demande de révocation usurpée avec signature valide, cela signifie que la clé privée est compromise et le certificat doit donc être révoqué.

Plateau du Moulon
3, rue Joliot-Curie
91192 Gif-sur-Yvette cedex
Tél: + 33 [0]1 69 85 12 12

Les noms et les coordonnées de ces personnes nommées spécifiquement sont renvoyés en annexe de la convention de délégation.

Une adresse électronique de support utilisateur igc-support-gif@supelec.fr permet aussi de réaliser des demandes de révocation par email.

5.2 Disponibilité

L'utilisateur qui désire obtenir un certificat remplit un formulaire en ligne sur le site WEB de l'IGC pilote du CRU : cette première étape peut être effectuée 24h/24 7j/7 sauf incident.

La demande est placée dans une file d'attente et les Opérateurs d'Enregistrement de SUPELEC-GIF sont prévenus par courrier électronique et dérouleront la procédure le plus tôt possible compte tenu de leurs autres fonctions et des possibilités d'établir un rendez-vous « de visu » avec le demandeur : il est raisonnable de signaler que, en pratique, les Opérateurs d'Enregistrement feront « de leur mieux » pour valider une demande de certificat le plus rapidement possible.

Le demandeur d'une révocation de certificat peut utiliser l'adresse électronique à disposition ou par FAX 24H/24 7j/7 (sauf incident). Les contacts « de visu » ou par téléphone se feront selon les disponibilités des Opérateurs d'Enregistrement, toujours en faisant « de leur mieux » pour traiter au plus vite la demande.

6 Support utilisateur

Il est assuré en premier lieu par courrier électronique à l'adresse igc-support-gif@supelec.fr et par téléphone auprès de la personne identifiée comme « support utilisateur » de l'IGC pilote du CRU.