To be filled out in the EDPS' office

REGISTER NUMBER: 74

NOTIFICATION FOR PRIOR CHECKING

Date of submission: 21/12/2005

Case number: 2005/410

Institution: COMMISSION

Legal basis: article 27-5 of the regulation CE 45/2001(1)

(1) OJ L 8, 12.01.2001

INFORMATION TO BE GIVEN(2)

(2) Please attach all necessary backup documents

1/ Name and adress of the controller

Name and First Name of the Controller:VERVAET Guido

Title:Head of Unit

Directorate, Unit or Service to which the Controller is attached:G.05

Directorate General to which the Controller is attached:ADMIN

2/ Organisational parts of the institution or body entrusted with the processing of personal data

External Company or Directorate, Unit or Service to which the Processor is attached:

External Company or Directorate General to which the Processor is attached:

3/ Name of the processing

PKI CommisSign - Génération et conservation des clés privées

4/ Purpose or purposes of the processing

Le système PKI de la Commission sert à l'identification et l'authentification de la personne à laquelle sont délivrés les clés et les certificats. Les applications sont par exemple l'encryption et la signature de messages électroniques (SECEM).
A l'exception de la copie de la clé privée d'encryption, qui est gardée dans un endroit spécifique et sécurisé (le serveur CA) et destinée à la récupération des données encryptées en cas de force majeure, les autres informations collectées sur la personne n'excèdent pas ce qui est strictement nécessaire au fonctionnement du système, à savoir le nom, le prénom, le userid et l'adresse email, informations qui sont déjà présentes dans le système de messagerie standard de la Commission et nécessaires dans le certificat afin de permettre l'intégration dans celui-ci.
Ci-jointe la procédure de recouvrement des clés privées d'encryption (en anglais).

5/ Description of the category or categories of data subjects

Data Subject(s) concerned:

Tout fonctionnaire ou personne ayant un lien contractuel avec la Commission (agent temporaire, contractuel, externe travaillant intra-muros) peut demander à son LISO l'autorisation d'utiliser SECEM et donc avoir besoin des clés et certificats générés par CommisSign. Une personne extérieure, moyennant la signature d'une déclaration d'acceptation de la politique de sécurité et l'accord du LISO peut également recevoir des clés et certificats CommiSsign.

Category(ies) of Data Subjects:

Il n'y a pas de catégories spéciales.

6/ Description of the data or categories of data*(including, if applicable, special categories of data (article 10) and/or origin of data)*

Data field(s) of Data Subjects: Attention: Please indicate and describe in the answer to this question also data fields which fall under article 10

Nom, prénom, userid, email.
Copie de la clé privée d'encryption.

Category(ies) of data fields of Data Subjects: Attention: Please indicate and describe in the answer to this question also categories of data fields which fall under article 10

2 catégories d'information sont enregistrées:
1. l'identité de la personne (nom, prénom, email, userid)
2. la clé privée d'encryption, permettant la récupération de données encryptées en cas de force majeure.

7/ Information to be given to data subjects

Which kind of communication(s) have you foreseen to inform the Data Subjects as described in articles 11 - 12 under 'Information to be given to the Data Subject'

Une interface Web permettant à l'utilisateur de s'enregistrer et de gérer ses clés et certificats est en cours de développement (mise en production 2006). Celle-ci comprendra un lien vers une page d'information de l'utilisateur.
En attendant les pages web, un complément d'information est ajouté sur les lettres d'accompagnement des codes reprenant le responsable du traitement, la finalité et les destinataires des données.
D'autre part, une formation destinée aux utilisateurs est disponible au Forum informatique. Celle-ci explique le concept de cryptographie à clé publique/privée et les risques éventuels liés à la perte ou la compromission des clés.
Il faut noter que le choix de donner cette formation aux utilisateurs est du seul ressort de la DG, sous la responsabilité du LISO, du Directeur General ou de l'IRM.
Le Certificate Practice Statement (CPS) explique aussi quelles information sont publiques et fait référence au

8/ Procedures to grant rights of data subjects*(rights of access, to rectify, to block, to erase, to object)*

Which procedure(s) did you put in place to enable Data Subjects to exert their rights: access, verify, correct, etc., their Personal Data as described in articles 13 - 19 under 'Rights of the Data Subject' :

Les certificats sont disponibles dans le système de messagerie et sur le système de l'utilisateur. Lors de la création de ceux-ci, l'utilisateur peut en visualiser le contenu.
L'utilisateur peut révoquer ses clés à n'importe quel moment si il juge ne plus avoir besoin du système.
Pour la clé privée d'encryption, il n'y a pas de vérification ni de correction à prévoir.

9/ Automated / Manual processing operation

Description of Processing: Attention: Please describe in the answer to this question if you process personal data falling under article 27 "Prior-Checking (by the EDPS - European Data Protection Supervisor)"

SECEM (SECure EMail) est un service qui fournit toute l'infrastructure et les services nécessaires à l'envoi et la réception de messages électroniques signés et/ou encryptés.
Pour fonctionner, SECEM a besoin de paires de clés cryptographiques publiques et privées, ainsi que de certificats numériques attestant de l'identité de la personne et établissant le lien avec ses clés publiques. Ces certificats sont générés par l'infrastructure à clé publique (PKI - Public Key Infrastructure) CommisSign de la Commission.
Les clés privées sont générées sous le contrôle exclusif de l'utilisateur mais la clé privée d'encryption est archivée de façon centralisée sur le système CA (Certification Authorithy - autorité de certification) afin de permettre la récupération de messages encryptés de l'utilisateur en cas de force majeure.
Automated Processing operation(s):

voir pièce jointe au point 7 (PKI - Automated Processing operation description.doc)

Manual Processing operation(s):

Les codes nécessaires à la création des clés et à l'enregistrement dans le système sont envoyés par courier interne, par 2 chemins différents (un par le RA de la DS et un par le LRA de la DG). Ces lettres doivent être conservées par l'utilisateur. Aucune copie n'est conservée.

10/ Storage media of data

La copie de la clé privée d'encryption est gardée dans une base de donnée sur le système PKI (CA) (voir question 31 pour la sécurité de ce système).
Les certificats sont également dans la base de données et copiés dans le répertoire du système de messagerie.
Les clés privées et les certificats sont également stockés sur le PC de l'utilisateur (dans le keystore de windows, protégé par un mot de passe connu de l'utilisateur seul) et sur une disquette de sauvegarde si celui-ci a décidé d'en faire une copie (sous la forme d'un fichier encrypté, protégé par un mot de passe connu de l'utilisateur seul).

11/ Legal basis and lawfulness of the processing operation

Legal basis of Processing:

Décision de la Commission C(94) 2129 (COMMISSION DECISION of 8 September 1994 on the tasks of the Security Office) (http://intracomm.cec.eu-admin.net/digitline/u/services/security/dssi/decisions/charteen-bottom.htm)
Décision de la Commission C(95) 1510 (COMMISSION DECISION ON THE PROTECTION OF INFORMATION SYSTEMS) (http://intracomm.cec.eu-admin.net/digitline/u/services/security/dssi/decisions/c1510en-bottom.htm)

Lawfulness of Processing: Answering this question please also verify and indicate if your processing has to comply with articles 20 "Exemptions and restrictions" and 27 "Prior checking (by the EDPS)"

Le traitement est nécessaire à l'exécution d'une mission effectuée dans l'intérêt publique.
Il s'agit de la protection de données "sensibles, mais non classifiées" échangées via le système de messagerie de la Commission. La conservation de la clé privée d'encryption (key escrow) est justifiée par la récupération de données importantes en cas de force majeure.

12/ The recipients or categories of recipient to whom the data might be disclosed

Recipient(s) of the Processing:

L'identité de la personne, se trouvant dans les certificats est disponible à tous les utilisateurs du système SECEM.

Les clés privées sont uniquement disponibles pour l'utilisateur.
La copie de la clée privée d'encryption est uniquement disponible pour l'agent de recouvrement (key recovery agent), rôle qui est tenu par du personnel autorisé de la DS.

Category(ies) of recipients:

Les certificats sont disponibles à tous les utilisateurs du système SECEM.
L'utilisateur a le contrôle de ses certificats. Il peut donc les exporter ou les envoyer consciemment à n'importe qui en dehors de l'institution.
Le système PKI en lui même n'exporte pas les données.
La copie de la clé privée d'encryption n'est jamais exportée.

13/ retention policy of (categories of) personal data

Les certificats sont archivés car ils sont nécessaires pour valider les signatures même quand ils ont expiré. Les clés privées d'encryption sont également gardées car elle sont nécessaires pour décrypter des messages qui ont été créés pendant leur période de validité.
La période de conservation est de 30 ans et est indépendante de la fin de service ou de la révocation des certificats.

13 a/ time limits for blocking and erasure of the different categories of data
(on justified legitimate request from the data subject)
(Please, specify the time limits for every category, if applicable)

Time limit to block/erase data on justified legitimate request from the data subjects:

14/ Historical, statistical or scientific purposes
If you store data for longer periods than mentioned above, please specify, if applicable, why the data must be kept under a form which permits identification,

Historical, statistical or scientific purposes - If you store data for longer periods than mentioned above, please specify, if applicable, why the data must be kept under a form which permits identification:

15/ Proposed transfers of data to third countries or international organisations

Legal foundation of transfer: Only transfers to third party countries not subject to Directive 95/46/EC (Article 9) should be considered for this question. Please treat transfers to other community institutions and bodies and to member states under question 20.

Pas d'application

Category(ies) of Personal Data or Personal Data to be transferred:

Pas d'application

16/ The processing operation presents specific risk which justifies prior checking (*please describe*):

Description of Processing: Attention: Please describe in the answer to this question if you process personal data falling under article 27 "Prior-Checking (by the EDPS - European Data Protection Supervisor)"

SECEM (SECure EMail) est un service qui fournit toute l'infrastructure et les services nécessaires à l'envoi et la réception de messages électroniques signés et/ou encryptés.
Pour fonctionner, SECEM a besoin de paires de clés cryptographiques publiques et privées, ainsi que de certificats numériques attestant de l'identité de la personne et établissant le lien avec ses clés publiques. Ces certificats sont générés par l'infrastructure à clé publique (PKI - Public Key Infrastructure) CommisSign de la Commission.
Les clés privées sont générées sous le contrôle exclusif de l'utilisateur mais la clé privée d'encryption est archivée de façon centralisée sur le système CA (Certification Authorithy - autorité de certification) afin de permettre la récupération de messages encryptés de l'utilisateur en cas de force majeure.
Lawfulness of Processing: Answering this question please also verify and indicate if your processing has to comply with articles 20 "Exemptions and restrictions" and 27 "Prior checking (by the EDPS)"

Le traitement est nécessaire à l'exécution d'une mission effectuée dans l'intérêt publique.
Il s'agit de la protection de données "sensibles, mais non classifiées" échangées via le système de messagerie de la Commission. La conservation de la clé privée d'encryption (key escrow) est justifiée par la récupération de données importantes en cas de force majeure.

AS FORESEEN IN:

Article 27.2.(a)
Processing of data relating to health and to suspected offences, offences, criminal convictions or security measures,

Non applicable

Article 27.2.(b)
Processing operations intended to evaluate personal aspects relating to the data subject,

Non applicable

Article 27.2.(c)

Processing operations allowing linkages not provided for pursuant to national or Community legislation between data processed for different purposes,

Non applicable

Article 27.2.(d)

Processing operations for the purpose of excluding individuals from a right, benefit or contract,

Non applicable

Other (general concept in Article 27.1)

Les traitements de données à caractère personnel relatifs au système "PKI CommisSign - Génération et conservation des clés privées " sont soumis suivant les dispositions du présent paragraphe de l'article 27.

17/ Comments

Date of submission:

Comments if applicable:

Les procédures sont documentées sur le site de la DIGIT http://intracomm.cec.eu-admin.net/home/dgserv/digit/corporate_ict/infrastruct/corp_systems/secserv/index_en.htm

Do you publish / distribute / give access to one or more printed and/or electronic directories?
Personal Data contained in printed and/or electronic directories of users and access to such directories shall be limited to what is strictly necessary for the specific purposes of the directory.
If Yes, please explain what is applicable.

yes
Les données publiées dans les certificats le sont déjà dans le système de messagerie de la Commission. Le certificat est attaché à ces données dans le répertoire du système de messagerie.

Complementary information to the different points if applicable:

PLACE AND DATE:20/12/2005

DATA PROTECTION OFFICER: HILBERT Nico

INSTITUTION OR BODY:European Commission