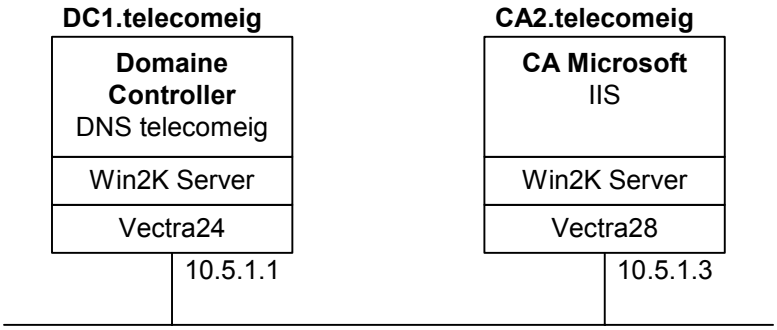
Mise en place d'une Entreprise Root CA Microsoft dans un domaine

1 Avant l'installation de la CA Microsoft

L'installation d'une Autorité de Certification (CA) ce fait sur une machine Windows 2000 server. Pour l'installation de Windows 2000 server, voir : Installation_Win2Kserver.doc.

Au moins un Contrôleur de Domaine (DC) avec Active Directory (AD) doit être présent dans le domaine. La CA et le DC peuvent être installés sur la même machine, mais dans notre cas, la CA est installée sur une machine séparée.

Le **serveur web IIS** doit être présent sur la machine avant l'installation de la CA. En effet, le support de requêtes de certificats ne sera pas installé sans IIS. Pour installer IIS : ***Start – Settings - Control Panel – Add/Remove Programs – Add/Remove Windows Components – Internet Information Services (IIS)***.



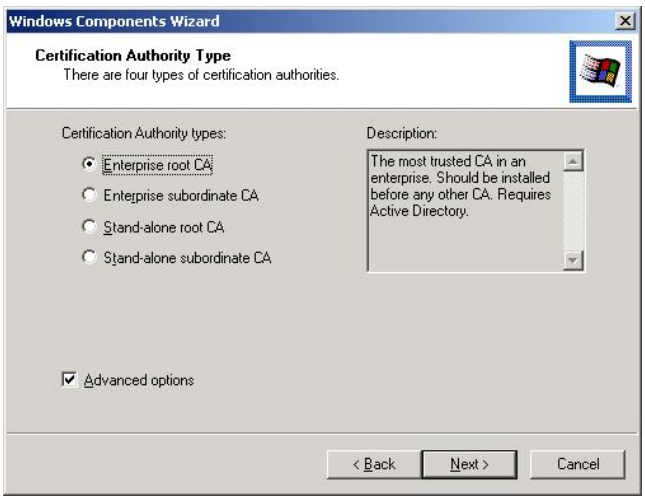
2 Installation de la CA

Pour installer la CA de Microsoft : ***Start – Settings - Control Panel – Add/Remove Programs – Add/Remove Windows Components – Certificate Services***.

2.1 Certification Authority Type

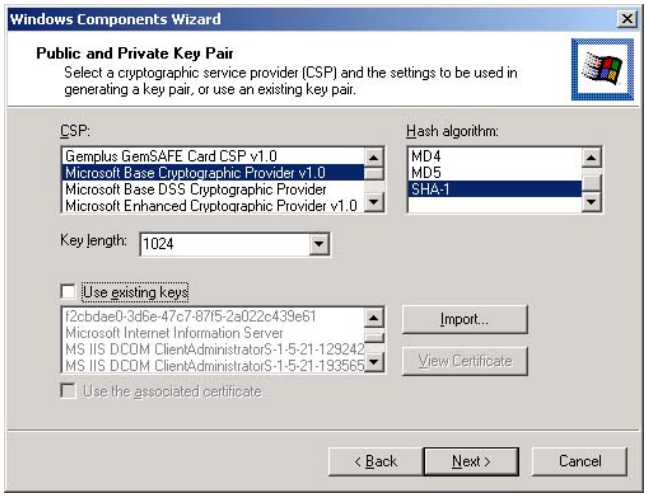
L'*Entreprise root CA* et l'*Entreprise subordinate CA* sont des CA intégré à un domaine Microsoft, c'est à dire à *Active Directory*. Ils nécessitent donc la présence d'un DC pour être installés. Le *Stand-alone root CA* et le *Stand-alone subordinate CA* peuvent être installés indépendamment d'un domaine.

Nous installons une *Entreprise root CA* pour qu'elle soit intégrée dans *Active Directory*.



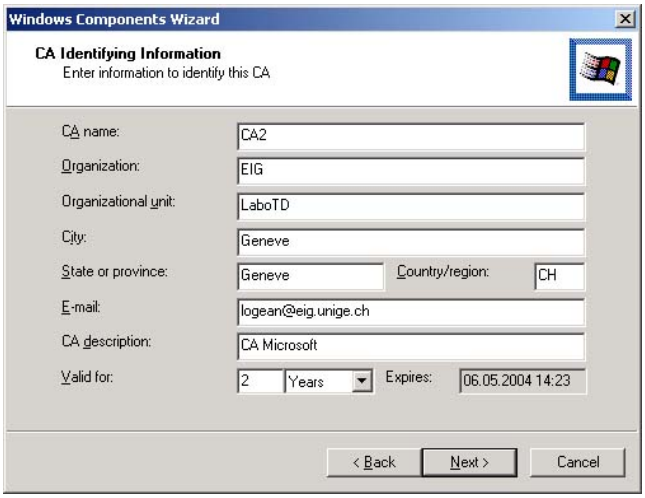
2.2 Public and Private Key Pair

Cette fenêtre apparaît si la coche ***Advanced options*** a été sélectionnée dans la fenêtre précédente. Elle permet de choisir le mode de génération de la clé privé et de la clé publique de la CA.



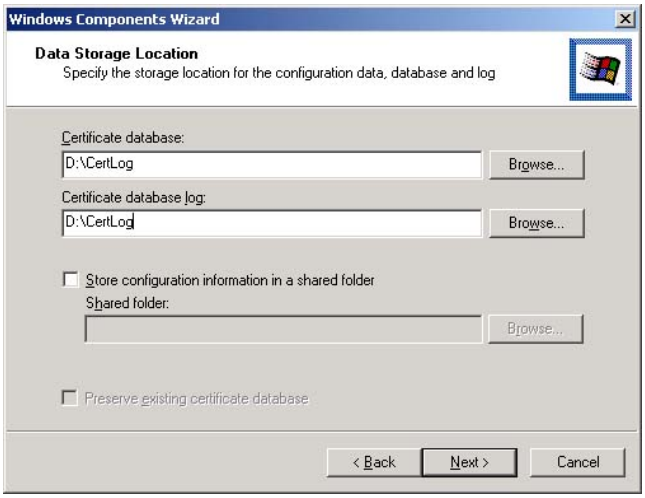
2.3 CA Identifying Information

Spécifier les informations permettant d'identifier la CA.



2.4 Data Storage Location

Dans cette fenêtre, on peut indiquer où sera stocker la base de donnée de la CA. Il est recommandé de la placer sur une partition différente que celle utilisée par Windows. En effet, en cas de réinstallation complète du serveur, la base de donnée ne sera pas perdue.



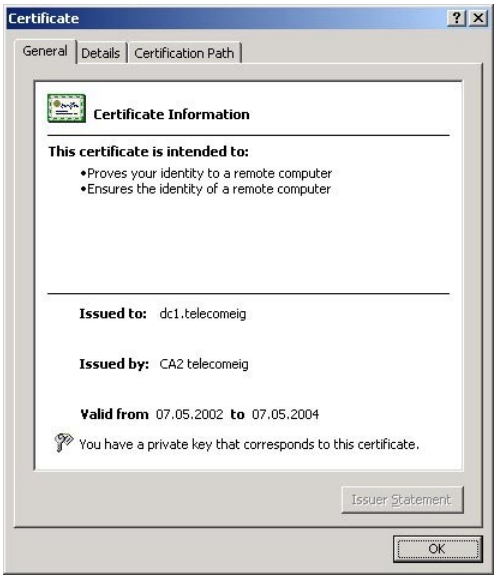
3 Après l'installation

Le certificat auto-signé de la CA (certificat root) se trouve dans C:\

A leur prochaine connexion, les machines Windows 2000 appartenant au domaine, vont obtenir ce certificat dans les *Trusted Root Certification Authorities*.

La CA est publiée dans *Active Directory* (dans LDAP://dc1.telecomeig/CN=NTAuthCertificats,CN=Public Key Services,CN=Services,CN=Configuration,DN=telecomeig) afin d'être reconnu comme *Enterprise Root CA*. Cela est nécessaire pour qu'elle soit reconnue comme une CA délivrant des certificats pour l'authentification des utilisateurs dans le domaine.

Un certificat est automatiquement délivrer au DC afin qu'il puisse signer ses échanges avec les clients. Il est parfois nécessaire de redémarrer le DC pour que ce certificat soit créé. **Sans ce certificat, l'authentification avec les *smartcards* ne fonctionne pas**.



La partie web permettant l'enregistrement (*enrollement*) se trouve dans C:\winnt\system32\certsrv\

Le lieu de stockage de la clef privé de la CA n'est pas déterminé. De plus il serait judicieux de faire un backup de cette clé (voir §8).

4 Certificate Templates

Les *certificate templates* sont des « modèles » de certificat prédéfinit contenant un certain nombre d'attribut. Certain de ces attributs sont obligatoires (*Issuer*, *Subject*, …) et d'autres sont des attributs d'extensions (*CA Version*, *Basic Constraints*, …). C'est ces attributs d'extensions qui différencient les *templates*. Ainsi, le CA va générer les certificats à partir de ces « modèles ».

4.1 Ajout de *Templates* sur la CA

Nous devons ajouter deux *templates* sur notre CA :

- *Enrollment Agent* : Permet de générer un certificat au nom d'un utilisateur, qui deviendra « agent d'enregistrement »
- *Smartcard User* : Permet de générer les certificats pour les utilisateurs, afin qu'ils puissent s'authentifier, lors du *login*, à l'aide de *smartcards* ou de *eTokens*

Pour cela il faut aller dans ***Start – Programs – Administrative Tools – Certification Authority – Policy Settings – New – Certificate to Issue*** et ajouter ***Enrollment Agent*** et ***Smartcard User***.

5 Mise en place de la station d'enregistrement (*Enrollment Station*) de *smart card*

La station d'enregistrement est la machine qui va nous permettre de délivrer des certificats aux utilisateurs du domaine afin qu'ils puissent être authentifier par le DC. Pour cela, les certificats seront installer sur des eToken Aladdin.

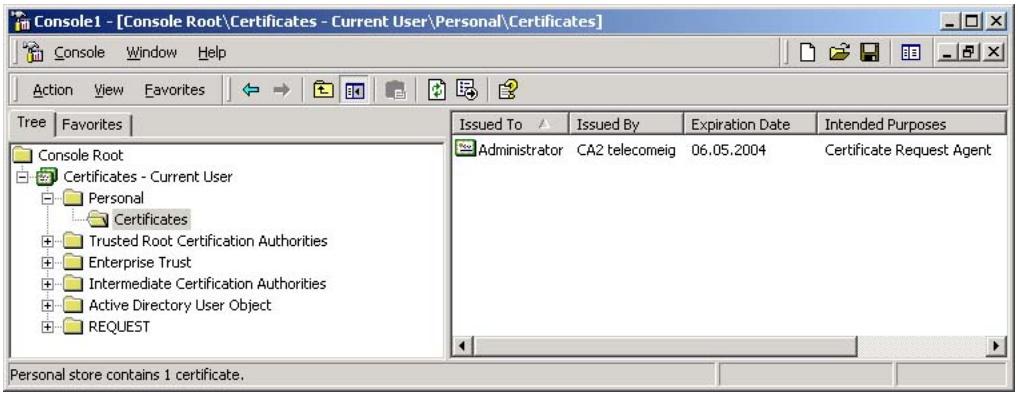
La personne qui est chargée de délivrer les certificats se nomme « agent d'enregistrement » (*Enrollment Agent*). Pour des raisons de sécurité, il est préférable que cet agent soit installé sur une seule machine dédiée à cette tache. De plus, cette machine devrait être accessible uniquement par l'agent d'enregistrement. Dans notre cas, l'agent d'enregistrement sera installé sur la même machine que la CA.

5.1 eToken Run Time Environement

Pour pouvoir utiliser les *eToken Aladdin* sur une machine, il faut installer le « *eToken Run Time Environement* ». Cela installe les drivers pour les *eToken*, le CSP « *eToken Base Cryptographic Provider* » et remplace la DLL GINA afin que les lecteurs de cartes à puces soient supporté par *Winlogon* . Le « *eToken Run Time Environement* » peux être téléchargé à l'adresse suivante :
http://www.ealaddin.com/etoken/downloads/rte.asp

5.2 Création de l'agent d'enregistrement (*Enrollment Agent*)

L'agent d'enregistrement est un utilisateur, ayant les droits d'administrateur, à qui on a délivré un certificat d'*Enrollment Agent*. Pour cela, il faut se loguer à la station d'enregistrement en utilisant le compte utilisateur choisi, puis ***Start – Run… - mmc – Console – Add/Remove Snap-in… - Add… - Certificates – Add – My user account***.

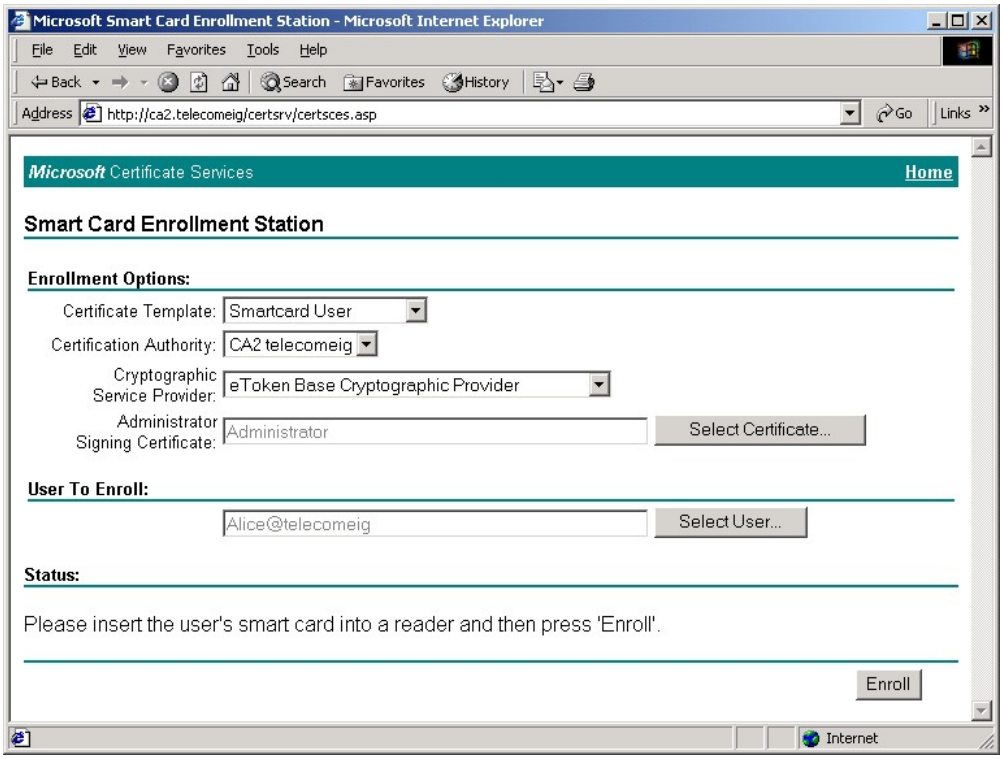


Dans le répertoire ***Personal***, faire ***All Tasks – Request New Certificate*** et sélectionner ***Enrollment Agent***. Le certificat est ainsi générer au nom de l'utilisateur. Pour terminer, Cliquer sur ***Install Certificate***.

6 Délivrer un certificat d'utilisateur sur un eToken Aladdin

Comme nous l'avons indiqué plus haut (§ 2.1), nous avons installé une *Entreprise Root CA*, qui est intégrée à *Active Directory*. Le but de cette CA est de pouvoir délivrer des certificats aux utilisateurs du domaine. Pour cela, elle va se baser sur la liste des utilisateurs disponible dans *Active Directory*. Cela implique que le contrôle de l'identité de l'utilisateur est délégué et effectué lors de l'enregistrement dans *Active Directory*.

Pour délivrer un certificat à un utilisateur du domaine, lancer Internet Explorer sur la station d'enregistrement et entrer l'adresse ***http://ca2.telecomeig/certsrv*** puis ***Request a certificate - Advanced request – Request a certificate for a smart card…*** .



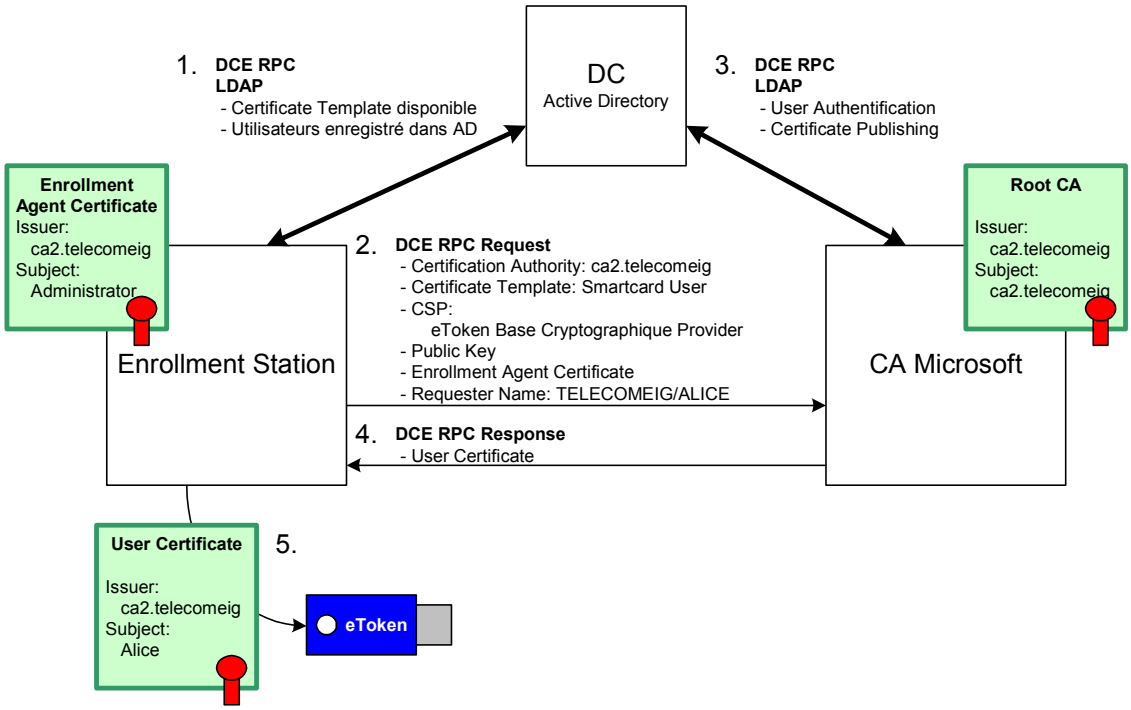
Vérifier qu'une *eToken* est bien connectée sur la station d'enregistrement.

- Dans ***Certificat Template***, mettre le modèle de certificat ***Smartcard User***.
- Indiquer la CA qui va délivrer le certificat dans ***Certification Authority***.
- Dans ***Cryptographic Service Provider***, mettre ***eTocken Base Cryptographic Provider***.
- Sélectionner le certificat de l'agent d'enregistrement dans ***Administrator Signing Certificate***.
- Enfin, choisire l'utilisateur destinataire du certificat (utilisateur présent dans *Active Directory*) dans ***User To Enroll***.
- Cliquer sur ***Enroll*** pour générer la paire de clé et le certificat dans la *eToken*.

Le PIN code de la *eToken* est demandé afin de pouvoir mémoriser la paire de clés générée.

6.1 Illustration de la procédure d'enregistrement

La figure ci-dessous montre le principe des échanges lors de la procédure d'enregistrement. Il est difficile d'entrer dans le détail, car à la différence d'une *CA Stand-alone* (qui respecte PKCS10 et PKCS7), *l'Entreprise Root CA* utilise un format qui lui est propre basé sur protocole DCE RPC (*Distributed Computing Environment Remote Procedure Call*).



- 1. Lorsque la page « *Smart Card Enrollment Station* » est ouvert dans le browser (§ 6), la station d'enregistrement effectue une requête sur le DC afin d'obtenir la liste des *certificate template* disponible et la liste des utilisateurs enregistrés dans AD.

- 2. Quand l'agent d'enregistrement appuie sur « *Enroll* », une paire de clé (publique et privé) est générée par le CSP sélectionné. Les données contenues dans les différant champs, ainsi que la clé publique générée et le certificat de l'agent d'enregistrement, sont envoyés à la CA (voir capture « *DCE RPC Request* » à la fin du document).

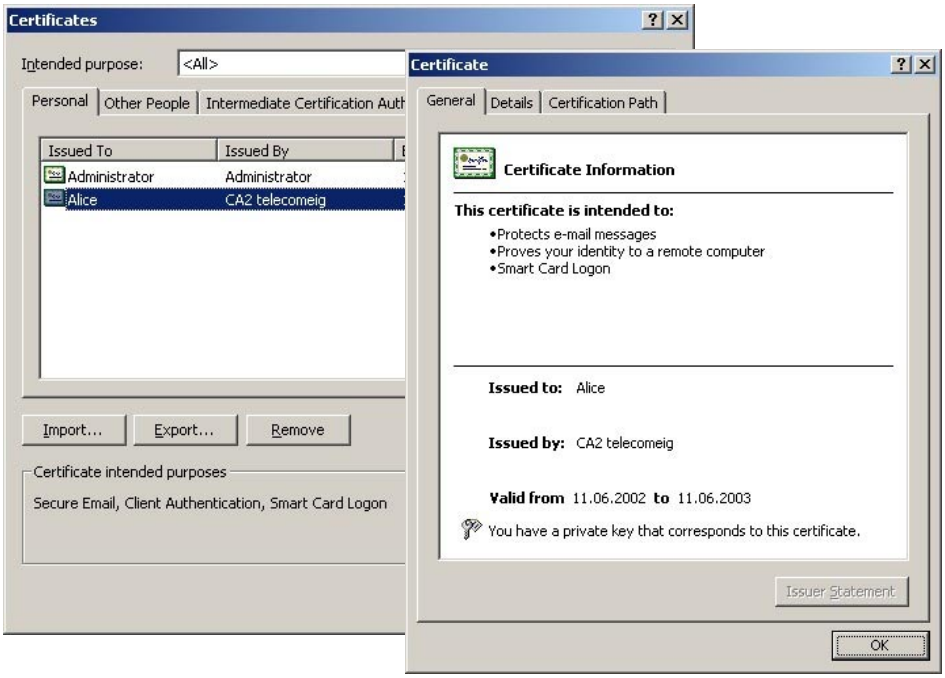
- 3. La CA vérifie l'authenticité des données reçues, génère et signe le certificat, puis le publie dans AD.

- 4. Le certificat de l'utilisateur est retourné à la station d'enregistrement (voir capture « *DCE RPC Response* » à la fin du document).

- 5. La clé privée et le certificat sont mémorisés dans la eToken.

6.2 Emplacement des clés générées

La clé privée et le certificat de l'utilisateur sont stockés dans la *eToken*. Lorsque la *eToken* est connectée à un poste, le certificat qu'elle contient peut être visualisé dans ***Internet Options – Content – Certificates… - Personal***.

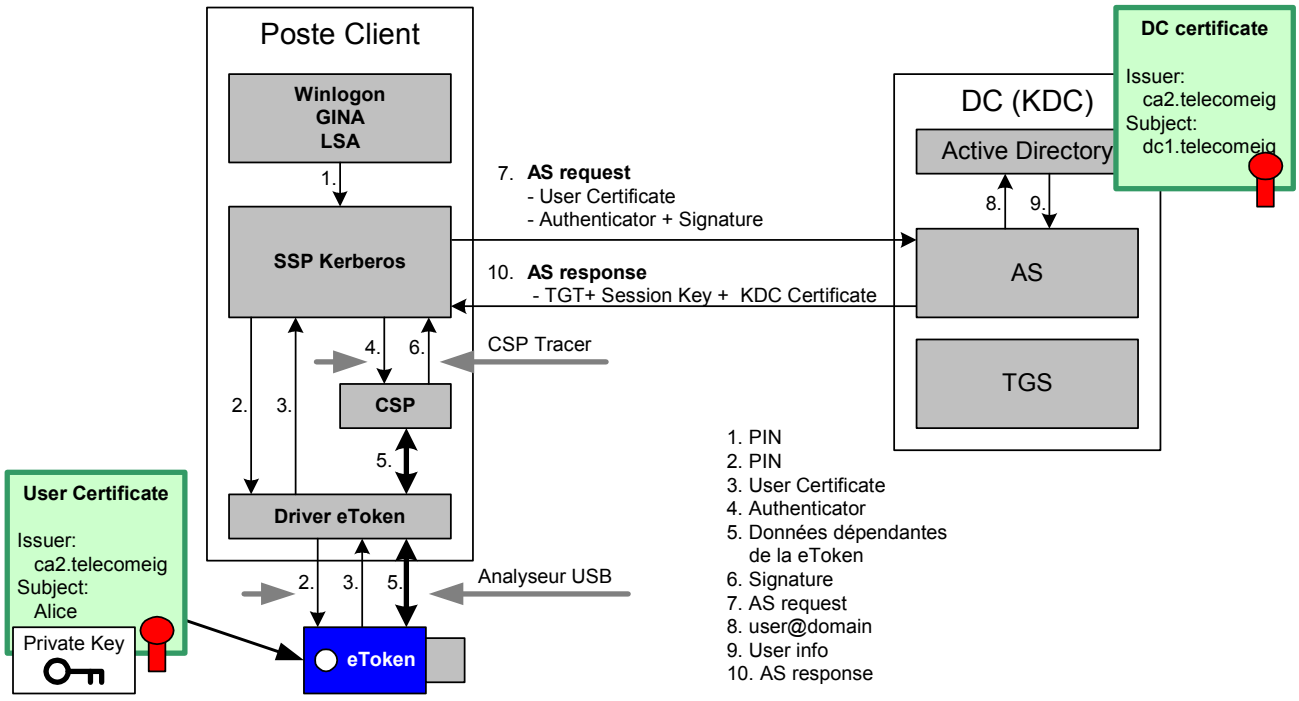


Remarque : Le certificat dans l'onglet ***Personal*** est un pointeur sur le certificat dans la *eToken*. Il reste visible même si la *eToken* est déconnecter du poste, mais n'est pas présent localement sur la machine.

7 Authentification d'un utilisateur avec une eToken Aladdin

La figure ci-dessous illustre le principe des échanges, à différent niveau, lors de l'authentification d'un utilisateur avec une eToken Aladdin. Pour mieux comprendre ce mécanisme, nous avons porté notre regard sur trois points :

- Echanges de paquets sur Ethernet, entre le client et le DC, avec un analyseur de protocoles.
- Echanges sur USB, entre la eToken et le poste client, avec un analyseur USB (USBShow v. 1.0.8).
- Appel d'API entre le SSP Kerberos et le CSP eToken, avec le CSP Tracer développé par Mario Pasquali lors de son travail de diplôme [W2kId].



7.1 Principe de l'authentification avec une eToken

- 1. Lorsqu'un utilisateur connecte une eToken sur le port USB d'un poste Win2K, *Winlogon* invite celui-ci à entrer son PIN (*Personal Identification Number*) afin de s'authentifier auprès de la carte à puce. Ce PIN est envoyé au SSP Kerberos par le LSA (*Local Security Authority*). Les mécanismes entre *Winlogon*, *MAGINA* et LSA sont décrit en détail dans le mémoire de diplôme de Mario Pasquali (p.18 [W2kId]).

- 2. Le SSP Kerberos effectue un appel au driver de la eToken et lui envoie le PIN afin d'accéder aux données contenues dans la carte à puce.

- 3. Le certificat de l'utilisateur est récupérer par le SSP.

- 4. Le SSP génère un authentifieur (*authenticator*) qui contient essentiellement l'heure (GMT) de la machine (*timestamp*) et l'envoie au CSP.

- 5.Cet authentifieur est signer avec la clé privée associer au certificat pour permettre au KDC d'authentifier l'utilisateur. Cette opération peut se faire de différentes manières suivant le type de eToken utilisée :
  - L'eToken R2 ne possède pas de processeur cryptographique. La clé privée est donc chargée sur le poste client et l'authentifieur est signer par le CPU local.
  - L'eToken Pro possède un processeur cryptographique. Le CSP envoie donc le *hash* (MD5) de l'authentifieur dans la eToken pour le signer. La signature est ensuite retournée au CSP. Ainsi, la clé privée n'est jamais copiée sur le poste client.

- 6. Le CSP retourne la signature au SSP Kerberos.

- 7. Le SSP envoie ensuite une requête AS (*Authentication Service*) au KDC du contrôleur de domaine pour obtenir un TGT (*Ticket Granting Ticket*). Le certificat est inclus dans les champs de pré-authentification de la requête AS ainsi que l'authentifieur et la signature.

Pour répondre à la requête AS, le KDC doit vérifier qu'il peut faire confiance aux CA contenues dans le chemin de certification (*Certification Path*) et que la CA root est bien publiée dans *NTAuthCertificates*. Le KDC retourne une erreur si le certificat root n'est pas crédible (*trusted*), s'il ne trouve pas les certificats des parents ou si la liste de révocation ne peut être déterminée.

Après cette vérification, le KDC utilise CryptoAPI pour vérifier la signature numérique de l'authentifieur avec la clé publique contenue dans le certificat. Le KDC doit encore valider le *timestamp* contenu dans l'authentifieur pour s'assurer que ce n'est pas une attaque de réplication.

- 8. Après avoir vérifié que l'utilisateur est bien celui qu'il prétend être, le KDC demande, au contrôleur de domaine, les informations du compte utilisateur correspondant au champ *Subject Alternative Name* du certificat (user@domain).

- 9. Les informations retournées (user SID (*Security Identifier*), user groups SID) sont utilisées pour construire le TGT. Ce dernier est chiffrer avec la clé du TGS puis signer par le KDC.

- 10. Le KDC retourne, au client, l'AS *response* qui contient le TGT, la clef de session client-TGS et le certificat du KDC. Cette réponse est chiffrée à l'aide d'une clé symétrique aléatoire (*random key*) qui est elle-même chiffré avec la clé publique du client. Le KDC signe cette réponse avec sa clé privée pour que le client puisse l'authentifier.

$$\mathrm{Sign}_{\mathrm{KDC\_Key}}\Big(\ \mathrm{Enc}_{\mathrm{Random\_Key}}\big[\ \mathrm{Sign}_{\mathrm{KDC\_Key}}(\ \mathrm{Enc}_{\mathrm{TGS\_Key}}[\ \mathbf{TGT}\ ]\ ),\ \mathbf{Session\_Key}\ ,\ \mathbf{Certif\_KDC}\ \big],\ \mathrm{ENC}_{\mathrm{Cpub\_Key}}[\ \mathbf{Random\_Key}\ ]\ \Big)$$

Le client peut déchiffrer la clé symétrique aléatoire avec sa clé privée et récupérer le TGT, la clé de session et le certificat du KDC. Ensuite, il vérifie le chemin de certification du certificat du KDC et authentifie la signature de la réponse. Lorsque le poste client est en possession du TGT, les demandes de tickets se font selon le protocole Kerberos standard. Pour plus d'informations sur ces échanges, voir le projet de semestre « Systèmes d'authentification » de Yann Souchon [SysAu].

7.2 Analyse des échanges

L'analyse des échanges lors de l'authentification d'un utilisateur avec une eToken n'est pas chose facile. En effet, il n'existe pas de décodeurs pour analyser les échange au niveau d'USB et du CSP. Au niveau d'Ethernet, les trames *AS_Req* et *AS_Resp* ne sont pas identiques aux trames standard Kerberos, donc non décodées. C'est pourquoi, il n'est pas possible de montrer des captures illustrant de manière clair les échanges décrit ci-dessus. Par contre, ces captures permettent de rechercher des éléments précis dans les trames hexadécimales, afin de vérifier certains éléments.

Les captures pour la eToken Pro se trouve dans Mesures\PKI\Capture CSP Logon Token Pro.
Les captures pour la eToken R2 se trouve dans Mesures\PKI\Capture CSP Logon Token R2.

Au niveau de la trace USB, l'échange du PIN et du certificat de l'utilisateur est visible.

Grâce au CSPTracer, on peut récupérer l'authentifieur envoyer par le SSP Kerberos au CSP (buffer HashData1.dat) :

```
Authenticator => 0U.S0Q..0........0...krbtgt..TELECOMEIG....TELECOMEIG.....6n.
                 ...20020702160339Z........
```

En procédant au hash MD5 de l'authentifieur, il est possible de le retrouver dans la trace USB effectuer avec la eToken Pro, mais pas dans celle effectuée avec la eToken R2. Cela prouve que, dans le premier cas, l'authentifieur est bien signer dans le eToken et, dans le deuxième, la signature se fait sur le post client.

Le CSPTracer montre aussi que les appels d'API, effectuer par le SSP Kerberos sur le CSP, sont exactement identiques pour les eToken Pro et R2.

CSPTracer nous a permit de constater que le certificat du KDC est chiffrer avec le TGT et la clé de session, lors de l'*AS_Resp* (buffer Decrypt0.dat). On voit, sur la trace ci-dessous, que la clé privée du client (pointeur 0x00000002) est utiliser pour déchiffrer et récupérer (*ImportKey*) la clé aléatoire (pointeur 0x000B95E0). Cette clé est ensuite utilisée pour décrypter le TGT, la clé de session et le certificat du KDC.

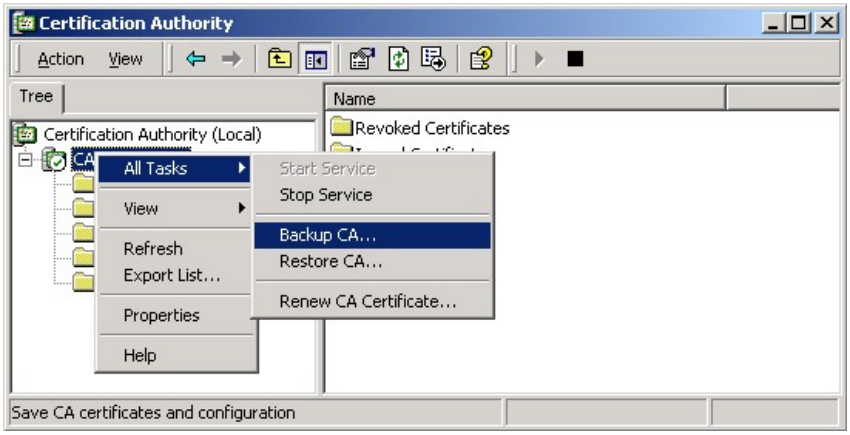
```
(CSP) GetUserKey(Provider: 0x000F3D88, KeySpec: 0x00000001, UserKey: 0x00000002)
(CSP) ImportKey(Provider: 0x000F3D88, PubKey: 0x00000002, Flags: 0x00000010, NewKey: 0x000B95E0)
      data saved in 'ImportKey0.dat'
(CSP) SetKeyParam(Provider: 0x000F3D88, Key: 0x000B95E0, Param: 0x00000001, Flags: 0x00000000)
(CSP) DestroyKey(Provider: 0x000F3D88, Key: 0x00000002)
(CSP) Decrypt(Provider: 0x000F3D88, Key: 0x000B95E0, Hash: 0x00000000, Final: 1, Flags:
      0x00000000) data saved in 'Decrypt0.dat'
(CSP) DestroyKey(Provider: 0x000F3D88, Key: 0x000B95E0)
```

Il est possible de retrouver ces éléments cryptés dans la trame *AS_Resp*.

8 Backup de la CA

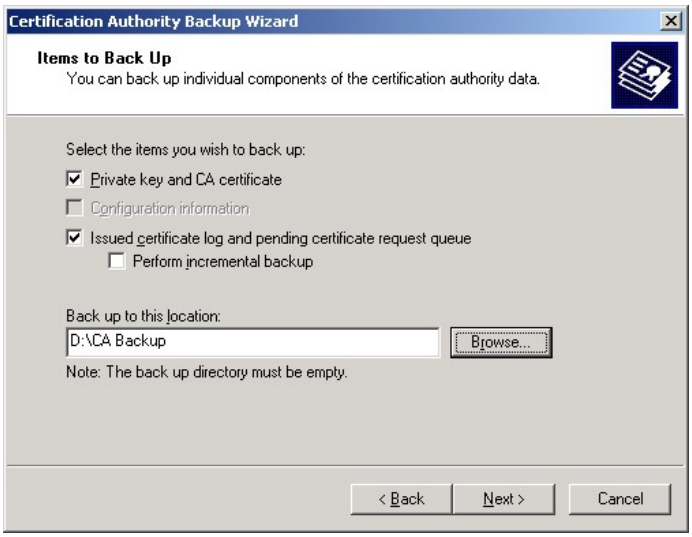
Le but du *backup* est de protéger la CA et sa base de donnée contre une perte accidentelle due à une panne de la machine où elle est installée. En effet, la perte de ces données remettrait en cause la validité de tous les certificats délivrés par cette CA. Cette opération permet de sauvegarder la clé privée, le certificat de la CA et la base de donnée de la CA.

Pour effectuer le *backup*, il faut aller dans ***Start – Programs – Administrative Tools – Certification Authority***, sélectionner la CA puis ***All Tasks – Backup CA…*** .



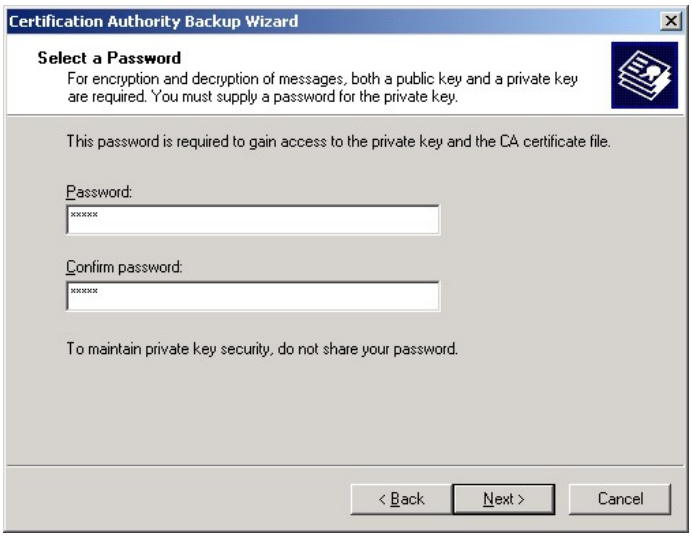
8.1 Items to Back Up

Cette boite de dialogue permet de sélectionner les éléments que l'on veut sauvegarder. En choisissant ***Perform incremtal backup***, seul les éléments modifiés, depuis le dernier *backup*, seront sauvegardés. Pour utiliser cette fonction, il faut déjà avoir préalablement sauvegarder la CA dans sont ensemble. Pour cela, on utilise la configuration ci-dessous. Indiquez le lieu où seront stockées les données.



8.2 Select a Password

Le certificat de la CA et la clé privé sont cryptés et stockés dans un fichier au format PKCS12. Entez un *password* permettant de récupérer ces fichiers lors de la restauration de la CA.



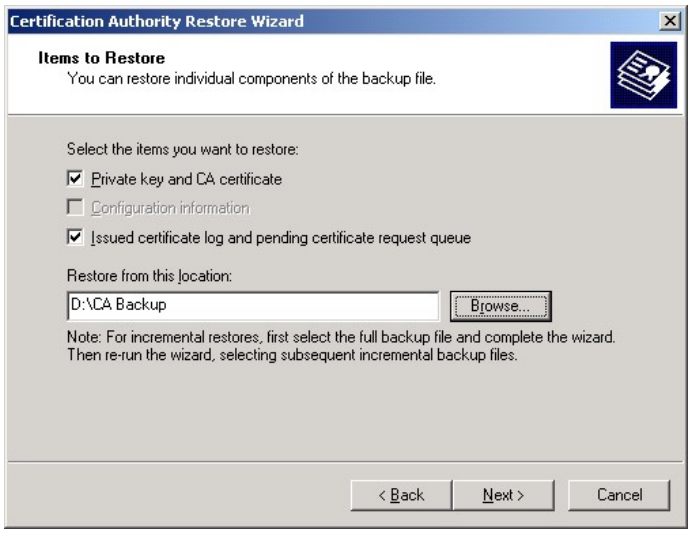
8.3 Sauvegarde des fichiers

Une fois le *backup* effectué, transférez les fichiers sur un support indépendant de la machine.
Conserver ces fichiers et le *password* en lieu sûr !!!

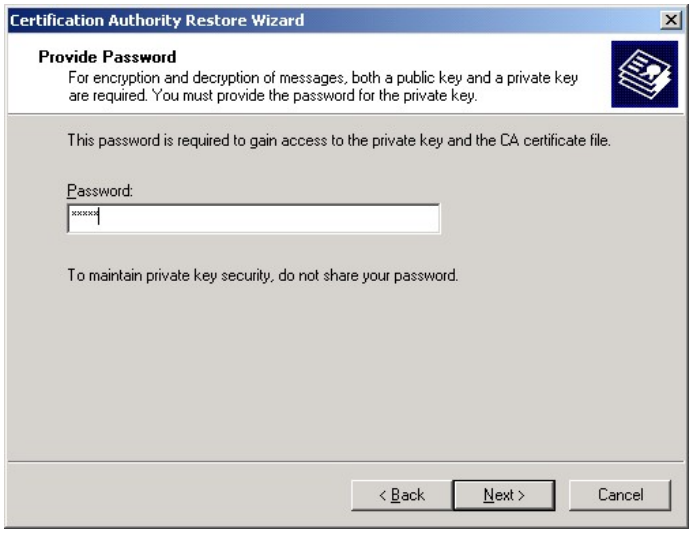
8.4 Restauration de la CA

Pour restaurer la CA, il faut aller dans ***Start – Programs – Administrative Tools – Certification Authority***, sélectionner la CA puis ***All Tasks – Restore CA…*** .

Sélectionnez les éléments à restaurer et indiquez le lieu où ils sont stockés



Entrez le *password* permettant d'extraire le certificat de la CA et la clé privé du fichier PKCS12.



Redémarrer la CA.

9 Sources

- **Windows 2000 Identification** (p. 19 - 24) [W2kId]
  Mémoire du travail de diplôme de Mario Pasquali
  Session 2001

- **Système d'authentification** (p. 3 - 7) [SysAu]
  Mémoire du projet de semestre de Yann Souchon
  Session 2001

- **Inside Windows 2000 Server** (p. 985 - 993) [InW2kS]
  William Boswell
  New Riders Publishing 2000, ISBN 1-56205-929-7

- **Microsoft Smart Card Logon White paper**
  Documentations\Pki\sclogonwp.doc

- **Troubleshooting Windows 2000 PKI Deployment and Smart Card Logon**
  Documentations\Pki\smrtcrdtrbl.doc

- **Microsoft Windows 2000 Kerberos Authentication White paper**
  Documentations\Pki\kerberos.doc

- **Deploying Smart Card**
  http://www.microsoft.com/technet/security/smrtcard/smartc09.asp

- **Integration Guide for Windows 2000 Smart Card Network Logon**
  Documentations\Pki\eToken + W2K SC Logon 2-5.pdf

- **Public Key Cryptography for Initial Authentication in Kerberos**
  Documentations\Pki\draft-ietf-cat-kerberos-pk-init-07.txt

- **Le système Kerberos**
  Documentations\Pki\L'Authentification - Réseaux et sécurité.htm

DCE RPC Request

```
Frame 31 (1514 on wire, 1514 captured)
    Arrival Time: Jun 11, 2002 16:25:42.845941000
    Time delta from previous packet: 0.000299000 seconds
    Time relative to first packet: 1.804426000 seconds
    Frame Number: 31
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
Ethernet II
    Destination: 00:04:76:9c:80:9c (ca2.telecomeig)
    Source: 00:04:76:9b:7a:ab (v26.telecomeig)
    Type: IP (0x0800)
Internet Protocol, Src Addr: v26.telecomeig (10.5.2.1), Dst Addr: ca2.telecomeig (10.5.1.3)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x294a
    Flags: 0x04
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (0x06)
    Header checksum: 0x0000 (incorrect, should be 0xb4c4)
    Source: v26.telecomeig (10.5.2.1)
    Destination: ca2.telecomeig (10.5.1.3)
Transmission Control Protocol, Src Port: 2071 (2071), Dst Port: 1037 (1037), Seq:
2136023680, Ack: 1491815833
    Source port: 2071 (2071)
    Destination port: 1037 (1037)
    Sequence number: 2136023680
    Next sequence number: 2136025140
    Acknowledgement number: 1491815833
    Header length: 20 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 17109
    Checksum: 0x1cdc (incorrect, should be 0x274e)
DCE RPC
    Version: 5
    Version (minor): 0
    Packet type: Request (0x00)
    Packet Flags: 0x03
        .... ...1 = First Frag: Set
        .... ..1. = Last Frag: Set
        .... .0.. = Cancel Pending: Not set
        .... 0... = Reserved: Not set
        ...0 .... = Multiplex: Not set
        ..0. .... = Did Not Execute: Not set
        .0.. .... = Maybe: Not set
        0... .... = Object: Not set
    Data Representation: 10000000
        Byte order: Little-endian (1)
        Character: ASCII (0)
        Floating-point: IEEE (0)
    Frag Length: 3173
    Auth Length: 37
    Call ID: 2
    Alloc hint: 3103
    Context ID: 1
    Opnum: 0
    Stub data (1436 bytes)
```

```
0000  00 04 76 9c 80 9c 00 04 76 9b 7a ab 08 00 45 00   ..v.....v.z...E.
0010  05 dc 29 4a 40 00 80 06 00 00 0a 05 02 01 0a 05   ..)J@...........
0020  01 03 08 17 04 0d 7f 51 22 80 58 eb 4d 99 50 10   .......Q".X.M.P.
0030  42 d5 1c dc 00 00 05 00 00 03 10 00 00 00 65 0c   B.............e.
0040  25 00 02 00 00 00 1f 0c 00 00 01 00 00 00 02 03   %...............
0050  00 00 90 31 0b 00 0f 00 00 00 00 00 00 00 0f 00   ...1............
0060  00 00 43 00 41 00 32 00 20 00 74 00 65 00 6c 00   ..C.A.2. .t.e.l.
0070  65 00 63 00 6f 00 6d 00 65 00 69 00 67 00 00 00   e.c.o.m.e.i.g...
0080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 d3 0b   ................
0090  00 00 70 03 18 02 d3 0b 00 00 30 82 0b cf 06 09   ..p.......0.....
00a0  2a 86 48 86 f7 0d 01 07 02 a0 82 0b c0 30 82 0b   *.H..........0..
00b0  bc 02 01 01 31 0b 30 09 06 05 2b 0e 03 02 1a 05   ....1.0...+.....
00c0  00 30 82 04 0c 06 09 2a 86 48 86 f7 0d 01 07 01   .0.....*.H......
00d0  a0 82 03 fd 04 82 03 f9 30 82 03 f5 30 82 03 9f   ........0...0...
00e0  02 01 00 30 00 30 5c 30 0d 06 09 2a 86 48 86 f7   ...0.0\0...*.H..
00f0  0d 01 01 01 05 00 03 4b 00 30 48 02 41 00 bb 17   .......K.0H.A...
0100  d1 90 3e 35 07 76 76 a6 30 58 6a a6 48 81 62 f6   ..>5.vv.0Xj.H.b.
0110  eb ac c6 2f 22 94 c7 8d f2 19 bf f7 ed f5 c0 8e   .../"...........
0120  d2 98 c8 92 71 1c 2f bb 3c 29 a6 bd 0b b6 0c 13   ....q./.<).......
0130  9a 7e 41 3a ea b1 09 05 fd c5 66 03 70 8d 02 03   .~A:......f.p...
0140  01 00 01 a0 82 03 38 30 1a 06 0a 2b 06 01 04 01   ......80...+....
0150  82 37 0d 02 03 31 0c 16 0a 35 2e 30 2e 32 31 39   .7...1...5.0.219
0160  35 2e 32 30 81 83 06 0a 2b 06 01 04 01 82 37 02   5.20....+.....7.
0170  01 0e 31 75 30 73 30 0e 06 03 55 1d 0f 01 01 ff   ..1u0s0...U.....
0180  04 04 03 02 04 f0 30 0b 06 03 55 1d 0f 04 04 03   ......0...U.....
0190  02 05 a0 30 29 06 03 55 1d 25 04 22 30 20 06 08   ...0)..U.%."0 ..
01a0  2b 06 01 05 05 07 03 04 06 08 2b 06 01 05 05 07   +.........+.....
01b0  03 02 06 0a 2b 06 01 04 01 82 37 14 02 02 30 29   ....+.....7...0)
01c0  06 09 2b 06 01 04 01 82 37 14 02 04 1c 1e 1a 00   ..+.....7.......
01d0  53 00 6d 00 61 00 72 00 74 00 63 00 61 00 72 00   S.m.a.r.t.c.a.r.
01e0  64 00 55 00 73 00 65 00 72 30 81 e7 06 0a 2b 06   d.U.s.e.r0....+.
01f0  01 04 01 82 37 0d 02 02 31 81 d8 30 81 d5 02 01   ....7...1..0....
0200  01 1e 44 00 65 00 54 00 6f 00 6b 00 65 00 6e 00   ..D.e.T.o.k.e.n.
0210  20 00 42 00 61 00 73 00 65 00 20 00 43 00 72 00    .B.a.s.e. .C.r.
0220  79 00 70 00 74 00 6f 00 67 00 72 00 61 00 70 00   y.p.t.o.g.r.a.p.
0230  68 00 69 00 63 00 20 00 50 00 72 00 6f 00 76 00   h.i.c. .P.r.o.v.
0240  69 00 64 00 65 00 72 03 81 89 00 27 d9 ee 7d 6b   i.d.e.r....'..}k
0250  7b 10 c4 4e 1e 32 44 09 64 85 23 73 96 1c f6 8f   {..N.2D.d.#s....
0260  85 54 f0 0d d9 87 54 e0 58 4c 50 9e a0 f6 c1 af   .T....T.XLP.....
0270  3b 8f b3 f9 74 8f b9 99 90 af de 7b 15 81 4c 71   ;...t......{..Lq
0280  20 d1 f2 e3 90 54 21 e4 ff 26 83 62 4c 88 f4 4e    ....T!..&.bL..N
0290  c7 22 bd 25 32 59 d3 de 54 1a 08 2d 97 d9 73 a9   .".%2Y..T..-..s.
02a0  09 11 82 38 cb 68 7d f6 2d ae 06 88 d1 2e e7 d2   ...8.h}.-.......
02b0  6f d4 6c 7e 17 f8 73 ab df ad b8 29 55 c1 ff 6b   o.l~..s....)U..k
02c0  48 10 82 97 19 e2 d5 e9 50 b5 8e 00 00 00 00 00   H.......P.......
02d0  00 00 00 30 82 01 a8 06 09 2a 86 48 86 f7 0d 01   ...0.....*.H....
02e0  09 0f 31 82 01 99 30 82 01 95 06 09 2a 86 48 86   ..1...0.....*.H.
02f0  f7 0d 01 07 02 a0 82 01 86 30 82 01 82 02 01 01   .........0......
0300  31 0b 30 09 06 05 2b 0e 03 02 1a 05 00 30 0b 06   1.0...+......0..
0310  09 2a 86 48 86 f7 0d 01 07 01 31 82 01 61 30 82   .*.H......1..a0.
0320  01 5d 02 01 01 30 14 30 00 02 10 a6 cf 3d 2d b4   .]...0.0.....=-.
0330  92 08 94 4a d5 25 8e e6 b5 90 b6 30 09 06 05 2b   ...J.%.....0...+
0340  0e 03 02 1a 05 00 a0 81 e5 30 18 06 09 2a 86 48   .........0...*.H
0350  86 f7 0d 01 09 03 31 0b 06 09 2a 86 48 86 f7 0d   ......1...*.H...
0360  01 07 01 30 1c 06 09 2a 86 48 86 f7 0d 01 09 05   ...0...*.H......
0370  31 0f 17 0d 30 32 30 36 31 31 31 34 32 35 33 39   1...020611142539
0380  5a 30 23 06 09 2a 86 48 86 f7 0d 01 09 04 31 16   Z0#..*.H......1.
0390  04 14 da 39 a3 ee 5e 6b 4b 0d 32 55 bf ef 95 60   ...9..^kK.2U...`
03a0  18 90 af d8 07 09 30 81 85 06 09 2a 86 48 86 f7   ......0....*.H..
03b0  0d 01 09 0f 31 78 30 76 30 0e 06 08 2a 86 48 86   ....1x0v0...*.H.
03c0  f7 0d 03 02 02 02 00 80 30 0e 06 08 2a 86 48 86   ........0...*.H.
03d0  f7 0d 03 04 02 02 00 80 30 07 06 05 2b 0e 03 02   ........0...+...
03e0  07 30 0a 06 08 2a 86 48 86 f7 0d 03 07 30 0b 06   .0...*.H.....0..
03f0  09 2a 86 48 86 f7 0d 01 01 05 30 0b 06 09 2a 86   .*.H......0...*.
0400  48 86 f7 0d 01 01 02 30 0b 06 09 2a 86 48 86 f7   H......0...*.H..
0410  0d 01 01 03 30 0b 06 09 2a 86 48 86 f7 0d 01 01   ....0...*.H.....
0420  04 30 0b 06 09 2a 86 48 86 f7 0d 01 01 01 30 0d   .0...*.H......0.
0430  06 09 2a 86 48 86 f7 0d 01 01 01 05 00 04 40 75   ..*.H.........@u
0440  39 ff 89 cc d1 ab 7b 7f 9a 91 05 fa b6 65 fc 7f   9.....{......e..
0450  f9 fc ea 63 ec 81 af ce 5f d0 e0 05 48 5a c1 57   ...c...._...HZ.W
```

Certification

Public Key

Certificate Template

CSP

```
0460  d4 34 21 47 f0 20 59 96 90 70 81 5c c7 3c 3d 30   .4!G. Y..p.\.<=0
0470  02 2c 62 13 f1 fb 5b ac be 41 1d 5a 96 09 8a 30   .,b...[..A.Z...0
0480  0d 06 09 2a 86 48 86 f7 0d 01 01 05 05 00 03 41   ...*.H.........A
0490  00 8b e3 d9 60 a8 90 b5 7b fa 77 cf 6f f0 bf 41   ....`...{.w.o..A
04a0  75 9e 3f f3 f5 70 8e 9b 0e ae d9 a3 c7 d9 11 e3   u.?..p..........
04b0  23 7e 38 c6 e0 74 77 bd a6 2e fb a1 46 dc 4b 51   #~8..tw.....F.KQ
04c0  1f ee 85 ab f3 0b cb de 5b 86 55 fe 1a 83 87 42   ........[.U....B
04d0  e7 a0 82 05 c4 30 82 05 c0 30 82 05 29 a0 03 02   .....0...0..)...
04e0  01 02 02 0a 01 45 fd f2 00 00 00 00 00 26 30 0d   .....E.......&0.
04f0  06 09 2a 86 48 86 f7 0d 01 01 05 05 00 30 81 88   ..*.H........0..
0500  31 1f 30 1d 06 09 2a 86 48 86 f7 0d 01 09 01 16   1.0...*.H.......
0510  10 6c 6f 67 65 61 6e 40 65 69 67 2e 75 6e 69 67   .logean@eig.unig
0520  65 31 0b 30 09 06 03 55 04 06 13 02 43 48 31 0f   e1.0...U....CH1.
0530  30 0d 06 03 55 04 08 13 06 47 65 6e 65 76 65 31   0...U....Geneve1
0540  0f 30 0d 06 03 55 04 07 13 06 47 65 6e 65 76 65   .0...U....Geneve
0550  31 0c 30 0a 06 03 55 04 0a 13 03 45 49 47 31 0f   1.0...U....EIG1.
0560  30 0d 06 03 55 04 0b 13 06 4c 61 62 6f 54 44 31   0...U....LaboTD1
0570  17 30 15 06 03 55 04 03 13 0e 43 41 32 20 74 65   .0...U....CA2 te
0580  6c 65 63 6f 6d 65 69 67 30 1e 17 0d 30 32 30 36   lecomeig0...0206
0590  31 30 31 32 32 35 32 30 5a 17 0d 30 34 30 35 30   10122520Z..04050
05a0  37 31 34 30 30 32 30 5a 30 18 31 16 30 14 06 03   7140020Z0.1.0...
05b0  55 04 03 13 0d 41 64 6d 69 6e 69 73 74 72 61 74   U....Administrat
05c0  6f 72 30 81 9f 30 0d 06 09 2a 86 48 86 f7 0d 01   or0..0...*.H....
05d0  01 01 05 00 03 81 8d 00 30 81 89 02 81 81 00 ca   ........0.......
05e0  72 60 9e be b3 ef 49 9f 13 3b                     r`....I..;
```

Enrollment Agent Certificate (partie 1)

Frame 32 (1514 on wire, 1514 captured)
- Arrival Time: Jun 11, 2002 16:25:42.845960000
- Time delta from previous packet: 0.000019000 seconds
- Time relative to first packet: 1.804445000 seconds
- Frame Number: 32
- Packet Length: 1514 bytes
- Capture Length: 1514 bytes

Ethernet II
- Destination: 00:04:76:9c:80:9c (ca2.telecomeig)
- Source: 00:04:76:9b:7a:ab (v26.telecomeig)
- Type: IP (0x0800)

Internet Protocol, Src Addr: v26.telecomeig (10.5.2.1), Dst Addr: ca2.telecomeig (10.5.1.3)
- Version: 4
- Header length: 20 bytes
- Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
  - 0000 00.. = Differentiated Services Codepoint: Default (0x00)
  - .... ..0. = ECN-Capable Transport (ECT): 0
  - ....0 = ECN-CE: 0
- Total Length: 1500
- Identification: 0x294b
- Flags: 0x04
  - .1.. = Don't fragment: Set
  - ..0. = More fragments: Not set
- Fragment offset: 0
- Time to live: 128
- Protocol: TCP (0x06)
- Header checksum: 0x0000 (incorrect, should be 0xb4c3)
- Source: v26.telecomeig (10.5.2.1)
- Destination: ca2.telecomeig (10.5.1.3)

Transmission Control Protocol, Src Port: 2071 (2071), Dst Port: 1037 (1037), Seq: 2136025140, Ack: 1491815833
- Source port: 2071 (2071)
- Destination port: 1037 (1037)
- Sequence number: 2136025140
- Next sequence number: 2136026600
- Acknowledgement number: 1491815833
- Header length: 20 bytes
- Flags: 0x0010 (ACK)
  - 0... .... = Congestion Window Reduced (CWR): Not set
  - .0.. .... = ECN-Echo: Not set
  - ..0. .... = Urgent: Not set
  - ...1 .... = Acknowledgment: Set
  - .... 0... = Push: Not set
  - .... .0.. = Reset: Not set
  - .... ..0. = Syn: Not set
  - ....0 = Fin: Not set
- Window size: 17109

Checksum: 0x1cdc (incorrect, should be 0x3252)

Data (1460 bytes)

```
0000  00 04 76 9c 80 9c 00 04 76 9b 7a ab 08 00 45 00   ..v.....v.z...E.
0010  05 dc 29 4b 40 00 80 06 00 00 0a 05 02 01 0a 05   ..)K@...........
0020  01 03 08 17 04 0d 7f 51 28 34 58 eb 4d 99 50 10   .......Q(4X.M.P.
0030  42 d5 1c dc 00 00 6e 0c 7a 78 34 ce 0f 3b 38 52   B.....n.zx4..;8R
0040  9f 15 64 3f 80 bd 50 de 88 2e 81 b1 10 f8 2e 21   ..d?..P........!
0050  8c e2 1b 36 b5 f0 87 00 71 b3 78 42 d9 c3 4b f6   ...6....q.xB..K.
0060  ce 4d d7 db 8a 81 e0 d6 e0 25 44 ef 2f f3 01 7b   .M.......%D./..{
0070  a6 24 06 4f e6 a8 5f 05 15 6c 8d 5d 67 6a a0 1c   .$.O.._..l.]gj..
0080  7c eb 77 89 73 86 e1 ed 92 51 28 e3 8e ef 42 f0   |.w.s....Q(...B.
0090  8c b3 01 98 b0 22 b1 35 3c a1 ab 89 13 37 5b a3   .....".5<....7[.
00a0  8a 19 1f 51 ea a5 d0 4f d6 5c 2f 02 03 01 00 01   ...Q...O.\/.....
00b0  a3 82 03 9e 30 82 03 9a 30 0b 06 03 55 1d 0f 04   ....0...0...U...
00c0  04 03 02 07 80 30 15 06 03 55 1d 25 04 0e 30 0c   .....0...U.%..0.
00d0  06 0a 2b 06 01 04 01 82 37 14 02 01 30 2d 06 09   ..+.....7...0-..
00e0  2b 06 01 04 01 82 37 14 02 04 20 1e 1e 00 45 00   +.....7... ...E.
00f0  6e 00 72 00 6f 00 6c 00 6c 00 6d 00 65 00 6e 00   n.r.o.l.l.m.e.n.
0100  74 00 41 00 67 00 65 00 6e 00 74 30 1d 06 03 55   t.A.g.e.n.t0...U
0110  1d 0e 04 16 04 14 e2 6b 03 46 ed e3 31 d4 99 a8   .......k.F..1...
0120  09 17 10 7c c1 d8 3f 2e e6 1e 30 81 c4 06 03 55   ...|..?...0....U
0130  1d 23 04 81 bc 30 81 b9 80 14 8f e8 ac 46 e9 51   .#...0.......F.Q
0140  f0 c7 37 ec 2b 34 c1 55 95 44 77 22 5e d9 a1 81   ..7.+4.U.Dw"^...
0150  8e a4 81 8b 30 81 88 31 1f 30 1d 06 09 2a 86 48   ....0..1.0...*.H
0160  86 f7 0d 01 09 01 16 10 6c 6f 67 65 61 6e 40 65   ........logean@e
0170  69 67 2e 75 6e 69 67 65 31 0b 30 09 06 03 55 04   ig.unige1.0...U.
0180  06 13 02 43 48 31 0f 30 0d 06 03 55 04 08 13 06   ...CH1.0...U....
0190  47 65 6e 65 76 65 31 0f 30 0d 06 03 55 04 07 13   Geneve1.0...U...
01a0  06 47 65 6e 65 76 65 31 0c 30 0a 06 03 55 04 0a   .Geneve1.0...U..
01b0  13 03 45 49 47 31 0f 30 0d 06 03 55 04 0b 13 06   ..EIG1.0...U....
01c0  4c 61 62 6f 54 44 31 17 30 15 06 03 55 04 03 13   LaboTD1.0...U...
01d0  0e 43 41 32 20 74 65 6c 65 63 6f 6d 65 69 67 82   .CA2 telecomeig.
01e0  10 16 e4 93 bc 07 07 b7 95 47 38 02 27 c4 b6 46   .........G8.'..F
01f0  49 30 82 01 03 06 03 55 1d 1f 04 81 fb 30 81 f8   I0.....U.....0..
0200  30 81 b8 a0 81 b5 a0 81 b2 86 81 af 6c 64 61 70   0...........ldap
0210  3a 2f 2f 2f 43 4e 3d 43 41 32 25 32 30 74 65 6c   :///CN=CA2%20tel
0220  65 63 6f 6d 65 69 67 2c 43 4e 3d 63 61 32 2c 43   ecomeig,CN=ca2,C
0230  4e 3d 43 44 50 2c 43 4e 3d 50 75 62 6c 69 63 25   N=CDP,CN=Public%
0240  32 30 4b 65 79 25 32 30 53 65 72 76 69 63 65 73   20Key%20Services
0250  2c 43 4e 3d 53 65 72 76 69 63 65 73 2c 43 4e 3d   ,CN=Services,CN=
0260  43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 2c 44 43   Configuration,DC
0270  3d 74 65 6c 65 63 6f 6d 65 69 67 3f 63 65 72 74   =telecomeig?cert
0280  69 66 69 63 61 74 65 52 65 76 6f 63 61 74 69 6f   ificateRevocatio
0290  6e 4c 69 73 74 3f 62 61 73 65 3f 6f 62 6a 65 63   nList?base?objec
02a0  74 63 6c 61 73 73 3d 63 52 4c 44 69 73 74 72 69   tclass=cRLDistri
02b0  62 75 74 69 6f 6e 50 6f 69 6e 74 30 3b a0 39 a0   butionPoint0;.9.
02c0  37 86 35 68 74 74 70 3a 2f 2f 63 61 32 2e 74 65   7.5http://ca2.te
02d0  6c 65 63 6f 6d 65 69 67 2f 43 65 72 74 45 6e 72   lecomeig/CertEnr
02e0  6f 6c 6c 2f 43 41 32 25 32 30 74 65 6c 65 63 6f   oll/CA2%20teleco
02f0  6d 65 69 67 2e 63 72 6c 30 82 01 12 06 08 2b 06   meig.crl0.....+.
0300  01 05 05 07 01 01 04 82 01 04 30 82 01 00 30 81   ..........0...0.
0310  ab 06 08 2b 06 01 05 05 07 30 02 86 81 9e 6c 64   ...+.....0....ld
0320  61 70 3a 2f 2f 2f 43 4e 3d 43 41 32 25 32 30 74   ap:///CN=CA2%20t
0330  65 6c 65 63 6f 6d 65 69 67 2c 43 4e 3d 41 49 41   elecomeig,CN=AIA
0340  2c 43 4e 3d 50 75 62 6c 69 63 25 32 30 4b 65 79   ,CN=Public%20Key
0350  25 32 30 53 65 72 76 69 63 65 73 2c 43 4e 3d 53   %20Services,CN=S
0360  65 72 76 69 63 65 73 2c 43 4e 3d 43 6f 6e 66 69   ervices,CN=Confi
0370  67 75 72 61 74 69 6f 6e 2c 44 43 3d 74 65 6c 65   guration,DC=tele
0380  63 6f 6d 65 69 67 3f 63 41 43 65 72 74 69 66 69   comeig?cACertifi
0390  63 61 74 65 3f 62 61 73 65 3f 6f 62 6a 65 63 74   cate?base?object
03a0  63 6c 61 73 73 3d 63 65 72 74 69 66 69 63 61 74   class=certificat
03b0  69 6f 6e 41 75 74 68 6f 72 69 74 79 30 50 06 08   ionAuthority0P..
03c0  2b 06 01 05 05 07 30 02 86 44 68 74 74 70 3a 2f   +.....0..Dhttp:/
03d0  2f 63 61 32 2e 74 65 6c 65 63 6f 6d 65 69 67 2f   /ca2.telecomeig/
03e0  43 65 72 74 45 6e 72 6f 6c 6c 2f 63 61 32 2e 74   CertEnroll/ca2.t
03f0  65 6c 65 63 6f 6d 65 69 67 5f 43 41 32 25 32 30   elecomeig_CA2%20
0400  74 65 6c 65 63 6f 6d 65 69 67 2e 63 72 74 30 42   telecomeig.crt0B
0410  06 03 55 1d 11 04 3b 30 39 a0 37 06 0a 2b 06 01   ..U...;09.7..+..
0420  04 01 82 37 14 02 03 a0 29 0c 27 41 64 6d 69 6e   ...7....).'Admin
0430  69 73 74 72 61 74 6f 72 40 74 65 6c 65 63 6f 6d   istrator@telecom
0440  65 69 67 00 00 44 43 3d 74 65 6c 65 63 6f 6d 65   eig..DC=telecome
0450  69 67 30 0d 06 09 2a 86 48 86 f7 0d 01 01 05 05   ig0...*.H.......
0460  00 03 81 81 00 7a 8d a5 5b c2 88 43 c5 28 cd 21   .....z..[..C.(.!
0470  15 f2 d4 9f fd c7 6b f1 df 6f e6 3a 5a 98 49 df   ......k..o.:Z.I.
```

Enrollment Agent Certificate (partie 2)

```
0480  cf 9a 99 4d 70 6c 7b 7b 36 d7 a3 f8 96 ad fe 3f   ...Mpl{{6......?
0490  95 fd 7c 4e 4a f7 45 9f ef 93 17 dd e8 06 8e 20   ..|NJ.E........
04a0  4d 3a aa 4f 95 3c 59 cc 84 4e ee d9 f6 f8 45 92   M:.O.<Y..N....E.
04b0  c5 93 48 b1 40 2b b6 60 fe 45 45 e7 4d 2a 0c a9   ..H.@+.`.EE.M*..
04c0  e3 67 30 ec 6c e7 d5 69 05 76 50 fc 27 7d c0 a7   .g0.l..i.vP.'}..
04d0  a9 91 5a fd a1 5e 99 46 38 c8 2b 21 3d ea 7f 58   ..Z..^.F8.+!=..X
04e0  94 13 c9 5f f6 31 82 01 d0 30 82 01 cc 02 01 01   ..._.1...0......
04f0  30 81 97 30 81 88 31 1f 30 1d 06 09 2a 86 48 86   0..0..1.0...*.H.
0500  f7 0d 01 09 01 16 10 6c 6f 67 65 61 6e 40 65 69   .......logean@ei
0510  67 2e 75 6e 69 67 65 31 0b 30 09 06 03 55 04 06   g.unige1.0...U..
0520  13 02 43 48 31 0f 30 0d 06 03 55 04 08 13 06 47   ..CH1.0...U....G
0530  65 6e 65 76 65 31 0f 30 0d 06 03 55 04 07 13 06   eneve1.0...U....
0540  47 65 6e 65 76 65 31 0c 30 0a 06 03 55 04 0a 13   Geneve1.0...U...
0550  03 45 49 47 31 0f 30 0d 06 03 55 04 0b 13 06 4c   .EIG1.0...U....L
0560  61 62 6f 54 44 31 17 30 15 06 03 55 04 03 13 0e   aboTD1.0...U....
0570  43 41 32 20 74 65 6c 65 63 6f 6d 65 69 67 02 0a   CA2 telecomeig..
0580  01 45 fd f2 00 00 00 00 00 26 30 09 06 05 2b 0e   .E.......&0...+.
0590  03 02 1a 05 00 a0 81 8f 30 18 06 09 2a 86 48 86   ........0...*.H.
05a0  f7 0d 01 09 03 31 0b 06 09 2a 86 48 86 f7 0d 01   .....1...*.H....
05b0  07 01 30 23 06 09 2a 86 48 86 f7 0d 01 09 04 31   ..0#..*.H......1
05c0  16 04 14 d2 03 ed ec 49 3b 5c 7f da f3 4c 26 e6   .......I;\...L&.
05d0  55 8d a7 82 30 70 c5 30 4e 06 0a 2b 06 01 04 01   U...0p.0N..+....
05e0  82 37 0d 02 01 31 40 30 3e 1e                     .7...1@0>.
```

Enrollment Agent Certificate (partie 3)

```
0000  00 04 76 9c 80 9c 00 04 76 9b 7a ab 08 00 45 00   ..v.....v.z...E.
0010  01 25 29 4c 40 00 80 06 00 00 0a 05 02 01 0a 05   .%)L@...........
0020  01 03 08 17 04 0d 7f 51 2d e8 58 eb 4d 99 50 18   .......Q-.X.M.P.
0030  42 d5 18 25 00 00 1a 00 52 00 65 00 71 00 75 00   B..%....R.e.q.u.
0040  65 00 73 00 74 00 65 00 72 00 4e 00 61 00 6d 00   e.s.t.e.r.N.a.m.
0050  65 1e 20 00 54 00 45 00 4c 00 45 00 43 00 4f 00   e. .T.E.L.E.C.O.
0060  4d 00 45 00 49 00 47 00 5c 00 41 00 6c 00 69 00   M.E.I.G.\.A.l.i.
0070  63 00 65 30 0d 06 09 2a 86 48 86 f7 0d 01 01 01   c.e0...*.H......
0080  05 00 04 81 80 84 61 1c 72 c8 2b 45 63 7a 6c b3   ......a.r.+Eczl.
0090  c5 ec 90 fa 2a db 24 b8 fd f0 c4 23 e0 3f 6a 71   ....*.$....#.?jq
00a0  55 33 92 aa f3 24 5a 72 86 e0 dc c1 f2 17 89 9c   U3...$Zr........
00b0  06 07 e7 58 6a b7 dc da 62 9d f4 f7 b6 04 e2 81   ...Xj...b.......
00c0  41 cf 4f 00 d8 fb 7f 1d dc 0b e3 22 21 70 2a 44   A.O........"!p*D
00d0  5f 84 2d 81 ad 3e 16 c1 a0 5c 8e 00 19 ee 3a 41   _.-..>...\....:A
00e0  e1 2b c0 54 ee e9 b2 b3 37 a4 3f b3 26 1c 20 ab   .+.T....7.?.&. .
00f0  1e 69 26 e3 97 1e 98 29 1f dc 4e 86 c7 e2 f2 bd   .i&....)..N.....
0100  98 ea 52 02 5c 20 09 05 01 00 98 05 16 02 60 23   ..R.\ ........`#
0110  06 09 2a 86 48 86 f7 12 01 02 02 01 01 11 00 ff   ..*.H...........
0120  ff ff ff 72 28 2c 55 bb d2 fe 61 37 bf 79 22 af   ...r(,U...a7.y".
0130  e1 92 cf                                          ...
```

Requester Name

```
Frame 33 (307 on wire, 307 captured)
    Arrival Time: Jun 11, 2002 16:25:42.845972000
    Time delta from previous packet: 0.000012000 seconds
    Time relative to first packet: 1.804457000 seconds
    Frame Number: 33
    Packet Length: 307 bytes
    Capture Length: 307 bytes
Ethernet II
    Destination: 00:04:76:9c:80:9c (ca2.telecomeig)
    Source: 00:04:76:9b:7a:ab (v26.telecomeig)
    Type: IP (0x0800)
Internet Protocol, Src Addr: v26.telecomeig (10.5.2.1), Dst Addr: ca2.telecomeig (10.5.1.3)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 293
    Identification: 0x294c
    Flags: 0x04
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (0x06)
    Header checksum: 0x0000 (incorrect, should be 0xb979)
    Source: v26.telecomeig (10.5.2.1)
    Destination: ca2.telecomeig (10.5.1.3)
Transmission Control Protocol, Src Port: 2071 (2071), Dst Port: 1037 (1037), Seq:
2136026600, Ack: 1491815833
    Source port: 2071 (2071)
    Destination port: 1037 (1037)
    Sequence number: 2136026600
    Next sequence number: 2136026853
    Acknowledgement number: 1491815833
    Header length: 20 bytes
    Flags: 0x0018 (PSH, ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 1... = Push: Set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 17109
    Checksum: 0x1825 (incorrect, should be 0x6acf)
Data (253 bytes)
```

DCE RPC Response

```
Frame 37 (1514 on wire, 1514 captured)
    Arrival Time: Jun 11, 2002 16:25:43.092739000
    Time delta from previous packet: 0.084895000 seconds
    Time relative to first packet: 2.051224000 seconds
    Frame Number: 37
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
Ethernet II
    Destination: 00:04:76:9b:7a:ab (v26.telecomeig)
    Source: 00:04:76:9c:80:9c (ca2.telecomeig)
    Type: IP (0x0800)
Internet Protocol, Src Addr: ca2.telecomeig (10.5.1.3), Dst Addr: v26.telecomeig (10.5.2.1)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        .... ...0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x1d08
    Flags: 0x04
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (0x06)
    Header checksum: 0xc106 (correct)
    Source: ca2.telecomeig (10.5.1.3)
    Destination: v26.telecomeig (10.5.2.1)
Transmission Control Protocol, Src Port: 1037 (1037), Dst Port: 2071 (2071), Seq:
1491815833, Ack: 2136026853
    Source port: 1037 (1037)
    Destination port: 2071 (2071)
    Sequence number: 1491815833
    Next sequence number: 1491817293
    Acknowledgement number: 2136026853
    Header length: 20 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        .... ...0 = Fin: Not set
    Window size: 17520
    Checksum: 0x4367 (correct)
DCE RPC
    Version: 5
    Version (minor): 0
    Packet type: Response (0x02)
    Packet Flags: 0x03
        .... ...1 = First Frag: Set
        .... ..1. = Last Frag: Set
        .... .0.. = Cancel Pending: Not set
        .... 0... = Reserved: Not set
        ...0 .... = Multiplex: Not set
        ..0. .... = Did Not Execute: Not set
        .0.. .... = Maybe: Not set
        0... .... = Object: Not set
    Data Representation: 10000000
        Byte order: Little-endian (1)
        Character: ASCII (0)
        Floating-point: IEEE (0)
    Frag Length: 4357
    Auth Length: 37
    Call ID: 2
    Alloc hint: 4284
    Context ID: 1
    Cancel count: 0
    Stub data (1436 bytes)
```

```
0000  00 04 76 9b 7a ab 00 04 76 9c 80 9c 08 00 45 00   ..v.z...v.....E.
0010  05 dc 1d 08 40 00 80 06 c1 06 0a 05 01 03 0a 05   ....@...........
0020  02 01 04 0d 08 17 58 eb 4d 99 7f 51 2e e5 50 10   ......X.M..Q..P.
0030  44 70 43 67 00 00 05 00 02 03 10 00 00 00 05 11   DpCg............
0040  25 00 02 00 00 00 bc 10 00 00 01 00 00 00 2e 00   %...............
0050  00 00 03 00 00 00 ac 09 00 00 08 10 52 01 ac 09   ............R...
0060  00 00 30 82 09 a8 06 09 2a 86 48 86 f7 0d 01 07   ..0.....*.H.....
0070  02 a0 82 09 99 30 82 09 95 02 01 01 31 00 30 0b   .....0......1.0.
0080  06 09 2a 86 48 86 f7 0d 01 07 01 a0 82 09 7d 30   ..*.H.........}0
0090  82 04 08 30 82 03 71 a0 03 02 01 02 02 10 16 e4   ...0..q.........
00a0  93 bc 07 07 b7 95 47 38 02 27 c4 b6 46 49 30 0d   ......G8.'..FI0.
00b0  06 09 2a 86 48 86 f7 0d 01 01 05 05 00 30 81 88   ..*.H........0..
00c0  31 1f 30 1d 06 09 2a 86 48 86 f7 0d 01 09 01 16   1.0...*.H.......
00d0  10 6c 6f 67 65 61 6e 40 65 69 67 2e 75 6e 69 67   .logean@eig.unig
00e0  65 31 0b 30 09 06 03 55 04 06 13 02 43 48 31 0f   e1.0...U....CH1.
00f0  30 0d 06 03 55 04 08 13 06 47 65 6e 65 76 65 31   0...U....Geneve1
0100  0f 30 0d 06 03 55 04 07 13 06 47 65 6e 65 76 65   .0...U....Geneve
0110  31 0c 30 0a 06 03 55 04 0a 13 03 45 49 47 31 0f   1.0...U....EIG1.
0120  30 0d 06 03 55 04 0b 13 06 4c 61 62 6f 54 44 31   0...U....LaboTD1
0130  17 30 15 06 03 55 04 03 13 0e 43 41 32 20 74 65   .0...U....CA2 te
0140  6c 65 63 6f 6d 65 69 67 30 1e 17 0d 30 32 30 35   lecomeig0...0205
0150  30 37 31 33 35 31 34 33 5a 17 0d 30 34 30 35 30   07135143Z..04050
0160  37 31 34 30 30 32 30 5a 30 81 88 31 1f 30 1d 06   7140020Z0..1.0..
0170  09 2a 86 48 86 f7 0d 01 09 01 16 10 6c 6f 67 65   .*.H........loge
0180  61 6e 40 65 69 67 2e 75 6e 69 67 65 31 0b 30 09   an@eig.unige1.0.
0190  06 03 55 04 06 13 02 43 48 31 0f 30 0d 06 03 55   ..U....CH1.0...U
01a0  04 08 13 06 47 65 6e 65 76 65 31 0f 30 0d 06 03   ....Geneve1.0...
01b0  55 04 07 13 06 47 65 6e 65 76 65 31 0c 30 0a 06   U....Geneve1.0..
01c0  03 55 04 0a 13 03 45 49 47 31 0f 30 0d 06 03 55   .U....EIG1.0...U
01d0  04 0b 13 06 4c 61 62 6f 54 44 31 17 30 15 06 03   ....LaboTD1.0...
01e0  55 04 03 13 0e 43 41 32 20 74 65 6c 65 63 6f 6d   U....CA2 telecom
01f0  65 69 67 30 81 9f 30 0d 06 09 2a 86 48 86 f7 0d   eig0..0...*.H...
0200  01 01 01 05 00 03 81 8d 00 30 81 89 02 81 81 00   .........0......
0210  bf 3a 28 73 00 16 99 22 e0 d9 22 cd 0f 6f be 6e   .:(s..."..".o.n
0220  2f 04 66 de 73 f9 88 20 0e 22 71 e6 bc d3 e8 6e   /.f.s.. ."q....n
0230  8c 71 be 01 65 5f 3f 11 89 cc 00 52 51 8d 4c bb   .q..e_?....RQ.L.
0240  65 84 ed 3a 5d 93 c1 10 af d6 e8 91 6f ec b1 2f   e..:].......o../
0250  6d fc 1a 7a ef 92 4a 16 70 7c ff 95 98 65 10 9b   m..z..J.p|...e..
0260  e3 01 73 ef e4 4e f1 8c d0 d0 c3 d5 56 76 57 cb   ..s..N......VvW.
0270  c8 de 20 c2 4f 8d d9 2c 1b 32 12 7e 18 fc 60 25   .. .O..,.2.~..`%
0280  0b 12 c7 f5 25 7f 9b da 02 e6 2a 2b bc c6 7c 97   ....%.....*+..|.
0290  02 03 01 00 01 a3 82 01 6f 30 82 01 6b 30 13 06   ........o0..k0..
02a0  09 2b 06 01 04 01 82 37 14 02 04 06 1e 04 00 43   .+.....7.......C
02b0  00 41 30 0b 06 03 55 1d 0f 04 04 03 02 01 46 30   .A0...U.......F0
02c0  0f 06 03 55 1d 13 01 01 ff 04 05 30 03 01 01 ff   ...U.......0....
02d0  30 1d 06 03 55 1d 0e 04 16 04 14 8f e8 ac 46 e9   0...U.........F.
02e0  51 f0 c7 37 ec 2b 34 c1 55 95 44 77 22 5e d9 30   Q..7.+4.U.Dw"^.0
02f0  82 01 03 06 03 55 1d 1f 04 81 fb 30 81 f8 30 81   .....U.....0..0.
0300  b8 a0 81 b5 a0 81 b2 86 81 af 6c 64 61 70 3a 2f   ..........ldap:/
0310  2f 2f 43 4e 3d 43 41 32 25 32 30 74 65 6c 65 63   //CN=CA2%20telec
0320  6f 6d 65 69 67 2c 43 4e 3d 63 61 32 2c 43 4e 3d   omeig,CN=ca2,CN=
0330  43 44 50 2c 43 4e 3d 50 75 62 6c 69 63 25 32 30   CDP,CN=Public%20
0340  4b 65 79 25 32 30 53 65 72 76 69 63 65 73 2c 43   Key%20Services,C
0350  4e 3d 53 65 72 76 69 63 65 73 2c 43 4e 3d 43 6f   N=Services,CN=Co
0360  6e 66 69 67 75 72 61 74 69 6f 6e 2c 44 43 3d 74   nfiguration,DC=t
0370  65 6c 65 63 6f 6d 65 69 67 3f 63 65 72 74 69 66   elecomeig?certif
0380  69 63 61 74 65 52 65 76 6f 63 61 74 69 6f 6e 4c   icateRevocationL
0390  69 73 74 3f 62 61 73 65 3f 6f 62 6a 65 63 74 63   ist?base?objectc
03a0  6c 61 73 73 3d 63 52 4c 44 69 73 74 72 69 62 75   lass=cRLDistribu
03b0  74 69 6f 6e 50 6f 69 6e 74 30 3b a0 39 a0 37 86   tionPoint0;.9.7.
03c0  35 68 74 74 70 3a 2f 2f 63 61 32 2e 74 65 6c 65   5http://ca2.tele
03d0  63 6f 6d 65 69 67 2f 43 65 72 74 45 6e 72 6f 6c   comeig/CertEnrol
03e0  6c 2f 43 41 32 25 32 30 74 65 6c 65 63 6f 6d 65   l/CA2%20telecome
03f0  69 67 2e 63 72 6c 30 10 06 09 2b 06 01 04 01 82   ig.crl0...+.....
0400  37 15 01 04 03 02 01 00 30 0d 06 09 2a 86 48 86   7.......0...*.H.
0410  f7 0d 01 01 05 05 00 03 81 81 00 4b ab 65 16 b8   ...........K.e..
0420  fa f1 fa 0a 45 96 b0 22 26 59 a5 3f 6d b3 be e3   ....E.."&Y.?m...
0430  59 cf 0d 64 07 22 1f 8d 8a 2c 4e 8a 3b 5d a1 12   Y..d."...,N.;]..
0440  0e 65 d7 16 01 ae 10 2e 79 ee 8b 9d ef 13 97 ed   .e......y.......
0450  53 13 f0 24 57 98 cb 7a 3e 61 25 04 f2 b3 0a b7   S..$W..z>a%.....
0460  1d d1 25 60 c1 dc 88 a7 9b 9d c5 81 ab cd 46 0d   ..%`..........F.
```

```
0470  f9 a0 ab c8 3d 46 32 43 b4 19 a1 79 bd 37 33 dc   ....=F2C...y.73.
0480  54 c1 03 02 bd 28 1c 76 b6 88 1d 8a 79 1d 23 2f   T....(.v....y.#/
0490  a4 c4 0d 96 ab 81 2b 7e 90 1c 02 30 82 05 6d 30   ......+~...0..m0
04a0  82 04 d6 a0 03 02 01 02 02 0a 06 d1 5f ce 00 00   ............_...
04b0  00 00 00 2e 30 0d 06 09 2a 86 48 86 f7 0d 01 01   ....0...*.H.....
04c0  05 05 00 30 81 88 31 1f 30 1d 06 09 2a 86 48 86   ...0..1.0...*.H.
04d0  f7 0d 01 09 01 16 10 6c 6f 67 65 61 6e 40 65 69   .......logean@ei
04e0  67 2e 75 6e 69 67 65 31 0b 30 09 06 03 55 04 06   g.unige1.0...U..
04f0  13 02 43 48 31 0f 30 0d 06 03 55 04 08 13 06 47   ..CH1.0...U....G
0500  65 6e 65 76 65 31 0f 30 0d 06 03 55 04 07 13 06   eneve1.0...U....
0510  47 65 6e 65 76 65 31 0c 30 0a 06 03 55 04 0a 13   Geneve1.0...U...
0520  03 45 49 47 31 0f 30 0d 06 03 55 04 0b 13 06 4c   .EIG1.0...U....L
0530  61 62 6f 54 44 31 17 30 15 06 03 55 04 03 13 0e   aboTD1.0...U....
0540  43 41 32 20 74 65 6c 65 63 6f 6d 65 69 67 30 1e   CA2 telecomeig0.
0550  17 0d 30 32 30 36 31 31 31 34 31 35 34 32 5a 17   ..020611141542Z.
0560  0d 30 33 30 36 31 31 31 31 34 31 35 34 32 5a 30   .030611141542Z0.
0570  31 0e 30 0c 06 03 55 04 03 13 05 41 6c 69 63 65   1.0...U....Alice
0580  30 5c 30 0d 06 09 2a 86 48 86 f7 0d 01 01 01 05   0\0...*.H.......
0590  00 03 4b 00 30 48 02 41 00 bb 17 d1 90 3e 35 07   ..K.0H.A.....>5.
05a0  76 76 a6 30 58 6a a6 48 81 62 f6 eb ac c6 2f 22   vv.0Xj.H.b..../"
05b0  94 c7 8d f2 19 bf f7 ed f5 c0 8e d2 98 c8 92 71   ...............q
05c0  1c 2f bb 3c 29 a6 bd 0b b6 0c 13 9a 7e 41 3a ea   ./.<).......~A:.
05d0  b1 09 05 fd c5 66 03 70 8d 02 03 01 00 01 a3 82   .....f.p........
05e0  03 97 30 82 03 93 30 0b 06 03                     ..0...0...
```

Frame 38 (1514 on wire, 1514 captured)
    Arrival Time: Jun 11, 2002 16:25:43.092862000
    Time delta from previous packet: 0.000123000 seconds
    Time relative to first packet: 2.051347000 seconds
    Frame Number: 38
    Packet Length: 1514 bytes
    Capture Length: 1514 bytes
Ethernet II
    Destination: 00:04:76:9b:7a:ab (v26.telecomeig)
    Source: 00:04:76:9c:80:9c (ca2.telecomeig)
    Type: IP (0x0800)
Internet Protocol, Src Addr: ca2.telecomeig (10.5.1.3), Dst Addr: v26.telecomeig (10.5.2.1)
    Version: 4
    Header length: 20 bytes
    Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
        0000 00.. = Differentiated Services Codepoint: Default (0x00)
        .... ..0. = ECN-Capable Transport (ECT): 0
        ....0 = ECN-CE: 0
    Total Length: 1500
    Identification: 0x1d09
    Flags: 0x04
        .1.. = Don't fragment: Set
        ..0. = More fragments: Not set
    Fragment offset: 0
    Time to live: 128
    Protocol: TCP (0x06)
    Header checksum: 0xc105 (correct)
    Source: ca2.telecomeig (10.5.1.3)
    Destination: v26.telecomeig (10.5.2.1)
Transmission Control Protocol, Src Port: 1037 (1037), Dst Port: 2071 (2071), Seq: 1491817293, Ack: 2136026853
    Source port: 1037 (1037)
    Destination port: 2071 (2071)
    Sequence number: 1491817293
    Next sequence number: 1491818753
    Acknowledgement number: 2136026853
    Header length: 20 bytes
    Flags: 0x0010 (ACK)
        0... .... = Congestion Window Reduced (CWR): Not set
        .0.. .... = ECN-Echo: Not set
        ..0. .... = Urgent: Not set
        ...1 .... = Acknowledgment: Set
        .... 0... = Push: Not set
        .... .0.. = Reset: Not set
        .... ..0. = Syn: Not set
        ....0 = Fin: Not set
    Window size: 17520
    Checksum: 0xbd2c (correct)

Data (1460 bytes)

```
0000  00 04 76 9b 7a ab 00 04 76 9c 80 9c 08 00 45 00   ..v.z...v.....E.
0010  05 dc 1d 09 40 00 80 06 c1 05 0a 05 01 03 0a 05   ....@...........
0020  02 01 04 0d 08 17 58 eb 53 4d 7f 51 2e e5 50 10   ......X.SM.Q..P.
0030  44 70 bd 2c 00 00 55 1d 0f 04 04 03 02 05 a0 30   Dp.,..U........0
0040  29 06 03 55 1d 25 04 22 30 20 06 08 2b 06 01 05   )..U.%."0 ..+...
0050  05 07 03 04 06 08 2b 06 01 05 05 07 03 02 06 0a   ......+.........
0060  2b 06 01 04 01 82 37 14 02 02 30 29 06 09 2b 06   +.....7...0)..+.
0070  01 04 01 82 37 14 02 04 1c 1e 1a 00 53 00 6d 00   ....7.......S.m.
0080  61 00 72 00 74 00 63 00 61 00 72 00 64 00 55 00   a.r.t.c.a.r.d.U.
0090  73 00 65 00 72 30 1d 06 03 55 1d 0e 04 16 04 14   s.e.r0...U......
00a0  88 bc 58 83 29 a5 fa 92 da 2a 2e c9 de 37 de 0a   ..X.)....*...7..
00b0  f6 b6 04 3e 30 81 c4 06 03 55 1d 23 04 81 bc 30   ...>0....U.#...0
00c0  81 b9 80 14 8f e8 ac 46 e9 51 f0 c7 37 ec 2b 34   .......F.Q..7.+4
00d0  c1 55 95 44 77 22 5e d9 a1 81 8e a4 81 8b 30 81   .U.Dw"^.......0.
00e0  88 31 1f 30 1d 06 09 2a 86 48 86 f7 0d 01 09 01   .1.0...*.H......
00f0  16 10 6c 6f 67 65 61 6e 40 65 69 67 2e 75 6e 69   ..logean@eig.uni
0100  67 65 31 0b 30 09 06 03 55 04 06 13 02 43 48 31   ge1.0...U....CH1
0110  0f 30 0d 06 03 55 04 08 13 06 47 65 6e 65 76 65   .0...U....Geneve
0120  31 0f 30 0d 06 03 55 04 07 13 06 47 65 6e 65 76   1.0...U....Genev
0130  65 31 0c 30 0a 06 03 55 04 0a 13 03 45 49 47 31   e1.0...U....EIG1
0140  0f 30 0d 06 03 55 04 0b 13 06 4c 61 62 6f 54 44   .0...U....LaboTD
0150  31 17 30 15 06 03 55 04 03 13 0e 43 41 32 20 74   1.0...U....CA2 t
0160  65 6c 65 63 6f 6d 65 69 67 82 10 16 e4 93 bc 07   elecomeig.......
0170  07 b7 95 47 38 02 27 c4 b6 46 49 30 82 01 03 06   ...G8.'..FI0....
0180  03 55 1d 1f 04 81 fb 30 81 f8 30 81 b8 a0 81 b5   .U.....0..0.....
0190  a0 81 b2 86 81 af 6c 64 61 70 3a 2f 2f 2f 43 4e   ......ldap:///CN
01a0  3d 43 41 32 25 32 30 74 65 6c 65 63 6f 6d 65 69   =CA2%20telecomei
01b0  67 2c 43 4e 3d 63 61 32 2c 43 4e 3d 43 44 50 2c   g,CN=ca2,CN=CDP,
01c0  43 4e 3d 50 75 62 6c 69 63 25 32 30 4b 65 79 25   CN=Public%20Key%
01d0  32 30 53 65 72 76 69 63 65 73 2c 43 4e 3d 53 65   20Services,CN=Se
01e0  72 76 69 63 65 73 2c 43 4e 3d 43 6f 6e 66 69 67   rvices,CN=Config
01f0  75 72 61 74 69 6f 6e 2c 44 43 3d 74 65 6c 65 63   uration,DC=telec
0200  6f 6d 65 69 67 3f 63 65 72 74 69 66 69 63 61 74   omeig?certificat
0210  65 52 65 76 6f 63 61 74 69 6f 6e 4c 69 73 74 3f   eRevocationList?
0220  62 61 73 65 3f 6f 62 6a 65 63 74 63 6c 61 73 73   base?objectclass
0230  3d 63 52 4c 44 69 73 74 72 69 62 75 74 69 6f 6e   =cRLDistribution
0240  50 6f 69 6e 74 30 3b a0 39 a0 37 86 35 68 74 74   Point0;.9.7.5htt
0250  70 3a 2f 2f 63 61 32 2e 74 65 6c 65 63 6f 6d 65   p://ca2.telecome
0260  69 67 2f 43 65 72 74 45 6e 72 6f 6c 6c 2f 43 41   ig/CertEnroll/CA
0270  32 25 32 30 74 65 6c 65 63 6f 6d 65 69 67 2e 63   2%20telecomeig.c
0280  72 6c 30 82 01 12 06 08 2b 06 01 05 05 07 01 01   rl0.....+.......
0290  04 82 01 04 30 82 01 00 30 81 ab 06 08 2b 06 01   ....0...0....+..
02a0  05 05 07 30 02 86 81 9e 6c 64 61 70 3a 2f 2f 2f   ...0....ldap:///
02b0  43 4e 3d 43 41 32 25 32 30 74 65 6c 65 63 6f 6d   CN=CA2%20telecom
02c0  65 69 67 2c 43 4e 3d 41 49 41 2c 43 4e 3d 50 75   eig,CN=AIA,CN=Pu
02d0  62 6c 69 63 25 32 30 4b 65 79 25 32 30 53 65 72   blic%20Key%20Ser
02e0  76 69 63 65 73 2c 43 4e 3d 53 65 72 76 69 63 65   vices,CN=Service
02f0  73 2c 43 4e 3d 43 6f 6e 66 69 67 75 72 61 74 69   s,CN=Configurati
0300  6f 6e 2c 44 43 3d 74 65 6c 65 63 6f 6d 65 69 67   on,DC=telecomeig
0310  3f 63 41 43 65 72 74 69 66 69 63 61 74 65 3f 62   ?cACertificate?b
0320  61 73 65 3f 6f 62 6a 65 63 74 63 6c 61 73 73 3d   ase?objectclass=
0330  63 65 72 74 69 66 69 63 61 74 69 6f 6e 41 75 74   certificationAut
0340  68 6f 72 69 74 79 30 50 06 08 2b 06 01 05 05 07   hority0P..+.....
0350  30 02 86 44 68 74 74 70 3a 2f 2f 63 61 32 2e 74   0..Dhttp://ca2.t
0360  65 6c 65 63 6f 6d 65 69 67 2f 43 65 72 74 45 6e   elecomeig/CertEn
0370  72 6f 6c 6c 2f 63 61 32 2e 74 65 6c 65 63 6f 6d   roll/ca2.telecom
0380  65 69 67 5f 43 41 32 25 32 30 74 65 6c 65 63 6f   eig_CA2%20teleco
0390  6d 65 69 67 2e 63 72 74 30 2b 06 03 55 1d 11 04   meig.crt0+..U...
03a0  24 30 22 a0 20 06 0a 2b 06 01 04 01 82 37 14 02   $0". ..+.....7..
03b0  03 a0 12 0c 10 41 6c 69 63 65 40 74 65 6c 65 63   .....Alice@telec
03c0  6f 6d 65 69 67 30 0d 06 09 2a 86 48 86 f7 0d 01   omeig0...*.H....
03d0  01 05 05 00 03 81 81 00 a1 53 4a 78 45 dc 47 46   .........SJxE.GF
03e0  a3 2b 3e c1 eb 0b 78 55 9c 51 15 73 05 3d 2b 13   .+>...xU.Q.s.=+.
03f0  53 4c 9e 50 ee 64 28 80 de 9c c0 f3 60 4b 01 68   SL.P.d(.....`K.h
0400  38 1b 06 34 d8 60 48 c0 36 fe a6 cb 40 5f aa 0c   8..4.`H.6...@_..
0410  54 b8 7d 84 ec ba 53 67 db 1b 05 ec ea 72 8b 2c   T.}...Sg.....r.,
0420  cc 7d e9 11 cf 44 cb 71 bf 32 26 83 d6 f8 52 0d   .}...D.q.2&...R.
0430  53 ff bc 02 bc 44 79 18 5f 0a 48 4e cb 04 03 15   S....Dy._.HN....
0440  bb 54 46 ee 61 b0 b8 36 6b a9 5d 29 ab f8 9a ad   .TF.a..6k.])....
0450  61 6e 31 6c b8 e6 93 13 31 00 71 05 00 00 c0 76   an1l....1.q....v
0460  16 00 71 05 00 00 30 82 05 6d 30 82 04 d6 a0 03   ..q...0..m0.....
0470  02 01 02 02 0a 06 d1 5f ce 00 00 00 00 00 2e 30   ......._.......0
0480  0d 06 09 2a 86 48 86 f7 0d 01 01 05 05 00 30 81   ...*.H........0.
```

```
0490  88 31 1f 30 1d 06 09 2a 86 48 86 f7 0d 01 09 01   .1.0...*.H......
04a0  16 10 6c 6f 67 65 61 6e 40 65 69 67 2e 75 6e 69   ..logean@eig.uni
04b0  67 65 31 0b 30 09 06 03 55 04 06 13 02 43 48 31   ge1.0...U....CH1
04c0  0f 30 0d 06 03 55 04 08 13 06 47 65 6e 65 76 65   .0...U....Geneve
04d0  31 0f 30 0d 06 03 55 04 07 13 06 47 65 6e 65 76   1.0...U....Genev
04e0  65 31 0c 30 0a 06 03 55 04 0a 13 03 45 49 47 31   e1.0...U....EIG1
04f0  0f 30 0d 06 03 55 04 0b 13 06 4c 61 62 6f 54 44   .0...U....LaboTD
0500  31 17 30 15 06 03 55 04 03 13 0e 43 41 32 20 74   1.0...U....CA2 t
0510  65 6c 65 63 6f 6d 65 69 67 30 1e 17 0d 30 32 30   elecomeig0...020
0520  36 31 31 31 34 31 35 34 32 5a 17 0d 30 33 30 36   611141542Z..0306
0530  31 31 31 34 31 35 34 32 5a 30 10 31 0e 30 0c 06   11141542Z0.1.0..
0540  03 55 04 03 13 05 41 6c 69 63 65 30 5c 30 0d 06   .U....Alice0\0..
0550  09 2a 86 48 86 f7 0d 01 01 01 05 00 03 4b 00 30   .*.H.........K.0
0560  48 02 41 00 bb 17 d1 90 3e 35 07 76 76 a6 30 58   H.A.....>5.vv.0X
0570  6a a6 48 81 62 f6 eb ac c6 2f 22 94 c7 8d f2 19   j.H.b..../".....
0580  bf f7 ed f5 c0 8e d2 98 c8 92 71 1c 2f bb 3c 29   ..........q./.<)
0590  a6 bd 0b b6 0c 13 9a 7e 41 3a ea b1 09 05 fd c5   .......~A:......
05a0  66 03 70 8d 02 03 01 00 01 a3 82 03 97 30 82 03   f.p..........0..
05b0  93 30 0b 06 03 55 1d 0f 04 04 03 02 05 a0 30 29   .0...U........0)
05c0  06 03 55 1d 25 04 22 30 20 06 08 2b 06 01 05 05   ..U.%."0 ..+....
05d0  07 03 04 06 08 2b 06 01 05 05 07 03 02 06 0a 2b   .....+.........+
05e0  06 01 04 01 82 37 14 02 02 30                     .....7...0
```

Frame 40 (1491 on wire, 1491 captured)
- Arrival Time: Jun 11, 2002 16:25:43.092979000
- Time delta from previous packet: 0.000095000 seconds
- Time relative to first packet: 2.051464000 seconds
- Frame Number: 40
- Packet Length: 1491 bytes
- Capture Length: 1491 bytes

Ethernet II
- Destination: 00:04:76:9b:7a:ab (v26.telecomeig)
- Source: 00:04:76:9c:80:9c (ca2.telecomeig)
- Type: IP (0x0800)

Internet Protocol, Src Addr: ca2.telecomeig (10.5.1.3), Dst Addr: v26.telecomeig (10.5.2.1)
- Version: 4
- Header length: 20 bytes
- Differentiated Services Field: 0x00 (DSCP 0x00: Default; ECN: 0x00)
  - 0000 00.. = Differentiated Services Codepoint: Default (0x00)
  - .... ..0. = ECN-Capable Transport (ECT): 0
  - ....0 = ECN-CE: 0
- Total Length: 1477
- Identification: 0x1d0a
- Flags: 0x04
  - .1.. = Don't fragment: Set
  - ..0. = More fragments: Not set
- Fragment offset: 0
- Time to live: 128
- Protocol: TCP (0x06)
- Header checksum: 0xc11b (correct)
- Source: ca2.telecomeig (10.5.1.3)
- Destination: v26.telecomeig (10.5.2.1)

Transmission Control Protocol, Src Port: 1037 (1037), Dst Port: 2071 (2071), Seq: 1491818753, Ack: 2136026853
- Source port: 1037 (1037)
- Destination port: 2071 (2071)
- Sequence number: 1491818753
- Next sequence number: 1491820190
- Acknowledgement number: 2136026853
- Header length: 20 bytes
- Flags: 0x0018 (PSH, ACK)
  - 0... .... = Congestion Window Reduced (CWR): Not set
  - .0.. .... = ECN-Echo: Not set
  - ..0. .... = Urgent: Not set
  - ...1 .... = Acknowledgment: Set
  - .... 1... = Push: Set
  - .... .0.. = Reset: Not set
  - .... ..0. = Syn: Not set
  - ....0 = Fin: Not set
- Window size: 17520
- Checksum: 0xc447 (correct)

Data (1437 bytes)

```
0000  00 04 76 9b 7a ab 00 04 76 9c 80 9c 08 00 45 00   ..v.z...v.....E.
0010  05 c5 1d 0a 40 00 80 06 c1 1b 0a 05 01 03 0a 05   ....@...........
0020  02 01 04 0d 08 17 58 eb 59 01 7f 51 2e e5 50 18   ......X.Y..Q..P.
0030  44 70 c4 47 00 00 29 06 09 2b 06 01 04 01 82 37   Dp.G..)..+.....7
0040  14 02 04 1c 1e 1a 00 53 00 6d 00 61 00 72 00 74   .......S.m.a.r.t
0050  00 63 00 61 00 72 00 64 00 55 00 73 00 65 00 72   .c.a.r.d.U.s.e.r
0060  30 1d 06 03 55 1d 0e 04 16 04 14 88 bc 58 83 29   0...U........X.)
0070  a5 fa 92 da 2a 2e c9 de 37 de 0a f6 b6 04 3e 30   ....*...7.....>0
0080  81 c4 06 03 55 1d 23 04 81 bc 30 81 b9 80 14 8f   ....U.#...0.....
0090  e8 ac 46 e9 51 f0 c7 37 ec 2b 34 c1 55 95 44 77   ..F.Q..7.+4.U.Dw
00a0  22 5e d9 a1 81 8e a4 81 8b 30 81 88 31 1f 30 1d   "^.......0..1.0.
00b0  06 09 2a 86 48 86 f7 0d 01 09 01 16 10 6c 6f 67   ..*.H........log
00c0  65 61 6e 40 65 69 67 2e 75 6e 69 67 65 31 0b 30   ean@eig.unige1.0
00d0  09 06 03 55 04 06 13 02 43 48 31 0f 30 0d 06 03   ...U....CH1.0...
00e0  55 04 08 13 06 47 65 6e 65 76 65 31 0f 30 0d 06   U....Geneve1.0..
00f0  03 55 04 07 13 06 47 65 6e 65 76 65 31 0c 30 0a   .U....Geneve1.0.
0100  06 03 55 04 0a 13 03 45 49 47 31 0f 30 0d 06 03   ..U....EIG1.0...
0110  55 04 0b 13 06 4c 61 62 6f 54 44 31 17 30 15 06   U....LaboTD1.0..
0120  03 55 04 03 13 0e 43 41 32 20 74 65 6c 65 63 6f   .U....CA2 teleco
0130  6d 65 69 67 82 10 16 e4 93 bc 07 07 b7 95 47 38   meig..........G8
0140  02 27 c4 b6 46 49 30 82 01 03 06 03 55 1d 1f 04   .'..FI0.....U...
0150  81 fb 30 81 f8 30 81 b8 a0 81 b5 a0 81 b2 86 81   ..0..0..........
0160  af 6c 64 61 70 3a 2f 2f 2f 43 4e 3d 43 41 32 25   .ldap:///CN=CA2%
0170  32 30 74 65 6c 65 63 6f 6d 65 69 67 2c 43 4e 3d   20telecomeig,CN=
0180  63 61 32 2c 43 4e 3d 43 44 50 2c 43 4e 3d 50 75   ca2,CN=CDP,CN=Pu
0190  62 6c 69 63 25 32 30 4b 65 79 25 32 30 53 65 72   blic%20Key%20Ser
01a0  76 69 63 65 73 2c 43 4e 3d 53 65 72 76 69 63 65   vices,CN=Service
01b0  73 2c 43 4e 3d 43 6f 6e 66 69 67 75 72 61 74 69   s,CN=Configurati
01c0  6f 6e 2c 44 43 3d 74 65 6c 65 63 6f 6d 65 69 67   on,DC=telecomeig
01d0  3f 63 65 72 74 69 66 69 63 61 74 65 52 65 76 6f   ?certificateRevo
01e0  63 61 74 69 6f 6e 4c 69 73 74 3f 62 61 73 65 3f   cationList?base?
01f0  6f 62 6a 65 63 74 63 6c 61 73 73 3d 63 52 4c 44   objectclass=cRLD
0200  69 73 74 72 69 62 75 74 69 6f 6e 50 6f 69 6e 74   istributionPoint
0210  30 3b a0 39 a0 37 86 35 68 74 74 70 3a 2f 2f 63   0;.9.7.5http://c
0220  61 32 2e 74 65 6c 65 63 6f 6d 65 69 67 2f 43 65   a2.telecomeig/Ce
0230  72 74 45 6e 72 6f 6c 6c 2f 43 41 32 25 32 30 74   rtEnroll/CA2%20t
0240  65 6c 65 63 6f 6d 65 69 67 2e 63 72 6c 30 82 01   elecomeig.crl0..
0250  12 06 08 2b 06 01 05 05 07 01 01 04 82 01 04 30   ...+...........0
0260  82 01 00 30 81 ab 06 08 2b 06 01 05 05 07 30 02   ...0....+.....0.
0270  86 81 9e 6c 64 61 70 3a 2f 2f 2f 43 4e 3d 43 41   ...ldap:///CN=CA
0280  32 25 32 30 74 65 6c 65 63 6f 6d 65 69 67 2c 43   2%20telecomeig,C
0290  4e 3d 41 49 41 2c 43 4e 3d 50 75 62 6c 69 63 25   N=AIA,CN=Public%
02a0  32 30 4b 65 79 25 32 30 53 65 72 76 69 63 65 73   20Key%20Services
02b0  2c 43 4e 3d 53 65 72 76 69 63 65 73 2c 43 4e 3d   ,CN=Services,CN=
02c0  43 6f 6e 66 69 67 75 72 61 74 69 6f 6e 2c 44 43   Configuration,DC
02d0  3d 74 65 6c 65 63 6f 6d 65 69 67 3f 63 41 43 65   =telecomeig?cACe
02e0  72 74 69 66 69 63 61 74 65 3f 62 61 73 65 3f 6f   rtificate?base?o
02f0  62 6a 65 63 74 63 6c 61 73 73 3d 63 65 72 74 69   bjectclass=certi
0300  66 69 63 61 74 69 6f 6e 41 75 74 68 6f 72 69 74   ficationAuthorit
0310  79 30 50 06 08 2b 06 01 05 05 07 30 02 86 44 68   y0P..+.....0..Dh
0320  74 74 70 3a 2f 2f 63 61 32 2e 74 65 6c 65 63 6f   ttp://ca2.teleco
0330  6d 65 69 67 2f 43 65 72 74 45 6e 72 6f 6c 6c 2f   meig/CertEnroll/
0340  63 61 32 2e 74 65 6c 65 63 6f 6d 65 69 67 5f 43   ca2.telecomeig_C
0350  41 32 25 32 30 74 65 6c 65 63 6f 6d 65 69 67 2e   A2%20telecomeig.
0360  63 72 74 30 2b 06 03 55 1d 11 04 24 30 22 a0 20   crt0+..U...$0".
0370  06 0a 2b 06 01 04 01 82 37 14 02 03 a0 12 0c 10   ..+.....7.......
0380  41 6c 69 63 65 40 74 65 6c 65 63 6f 6d 65 69 67   Alice@telecomeig
0390  30 0d 06 09 2a 86 48 86 f7 0d 01 01 05 05 00 03   0...*.H.........
03a0  81 81 00 a1 53 4a 78 45 dc 47 46 a3 2b 3e c1 eb   ....SJxE.GF.+>..
03b0  0b 78 55 9c 51 15 73 05 3d 2b 13 53 4c 9e 50 ee   .xU.Q.s.=+.SL.P.
03c0  64 28 80 de 9c c0 f3 60 4b 01 68 38 1b 06 34 d8   d(.....`K.h8..4.
03d0  60 48 c0 36 fe a6 cb 40 5f aa 0c 54 b8 7d 84 ec   `H.6...@_..T.}..
03e0  ba 53 67 db 1b 05 ec ea 72 8b 2c cc 7d e9 11 cf   .Sg.....r.,.}...
03f0  44 cb 71 bf 32 26 83 d6 f8 52 0d 53 ff bc 02 bc   D.q.2&...R.S....
0400  44 79 18 5f 0a 48 4e cb 04 03 15 bb 54 46 ee 61   Dy._.HN.....TF.a
0410  b0 b8 36 6b a9 5d 29 ab f8 9a ad 61 6e 31 6c b8   ..6k.])....anl1.
0420  e6 93 13 b4 7e 85 6a 01 00 00 80 55 13 00 6a 01   ....~.j....U..j.
0430  00 00 49 00 73 00 73 00 75 00 65 00 64 00 20 00   ..I.s.s.u.e.d. .
0440  20 00 54 00 68 00 65 00 20 00 45 00 6e 00 72 00    .T.h.e. .E.n.r.
0450  6f 00 6c 00 6c 00 65 00 65 00 20 00 28 00 43 00   o.l.l.e.e. .(.C.
0460  4e 00 3d 00 41 00 6c 00 69 00 63 00 65 00 2c 00   N.=.A.l.i.c.e.,.
0470  4f 00 55 00 3d 00 55 00 74 00 69 00 6c 00 69 00   O.U.=.U.t.i.l.i.
0480  73 00 61 00 74 00 65 00 75 00 72 00 73 00 20 00   s.a.t.e.u.r.s. .
0490  45 00 49 00 47 00 2c 00 44 00 43 00 3d 00 74 00   E.I.G.,.D.C.=.t.
04a0  65 00 6c 00 65 00 63 00 6f 00 6d 00 65 00 69 00   e.l.e.c.o.m.e.i.
```

```
04b0  67 00 29 00 20 00 68 00 61 00 73 00 20 00 6e 00   g.). .h.a.s. .n.
04c0  6f 00 20 00 45 00 2d 00 4d 00 61 00 69 00 6c 00   o. .E.-.M.a.i.l.
04d0  20 00 6e 00 61 00 6d 00 65 00 20 00 72 00 65 00    .n.a.m.e. .r.e.
04e0  67 00 69 00 73 00 74 00 65 00 72 00 65 00 64 00   g.i.s.t.e.r.e.d.
04f0  20 00 69 00 6e 00 20 00 74 00 68 00 65 00 20 00    .i.n. .t.h.e. .
0500  41 00 63 00 74 00 69 00 76 00 65 00 20 00 44 00   A.c.t.i.v.e. .D.
0510  69 00 72 00 65 00 63 00 74 00 6f 00 72 00 79 00   i.r.e.c.t.o.r.y.
0520  2e 00 20 00 20 00 54 00 68 00 65 00 20 00 45 00   .. . .T.h.e. .E.
0530  2d 00 4d 00 61 00 69 00 6c 00 20 00 6e 00 61 00   -.M.a.i.l. .n.a.
0540  6d 00 65 00 20 00 77 00 69 00 6c 00 6c 00 20 00   m.e. .w.i.l.l. .
0550  6e 00 6f 00 74 00 20 00 62 00 65 00 20 00 69 00   n.o.t. .b.e. .i.
0560  6e 00 63 00 6c 00 75 00 64 00 65 00 64 00 20 00   n.c.l.u.d.e.d. .
0570  69 00 6e 00 20 00 74 00 68 00 65 00 20 00 63 00   i.n. .t.h.e. .c.
0580  65 00 72 00 74 00 69 00 66 00 69 00 63 00 61 00   e.r.t.i.f.i.c.a.
0590  74 00 65 00 2e 00 0d 00 0a 00 00 00 54 00 00 00   t.e.........T...
05a0  00 00 20 00 45 00 09 05 04 00 98 05 16 02 60 23   .. .E.........`#
05b0  06 09 2a 86 48 86 f7 12 01 02 02 01 01 11 00 ff   ..*.H...........
05c0  ff ff ff 66 1a a5 c6 4c 9f 87 79 76 d1 49 7b 74   ...f...L..yv.I{t
05d0  e3 0f a3                                         ...
```

Clé publique d'ALICE