Un catalogue de services

Global One, Bruxelles, 2001

A Member of the France Telecom Group

Table des matières


Un catalogue
de services

Avant-propos

1

TESTA offre une infrastructure de télécommunications destinées aux administrations européennes. C'est un réseau privé pour des administrations publiques.

Les administrations publiques ont besoin d'accéder à des services de télécommunications modernes pour leurs opérations. Dans leurs activités quotidiennes, elles sont intégrées dans et s'appuient sur le bon fonctionnement d'un réseau de relations avec des citoyens, des entreprises, des organisations sans but lucratif et d'autres organismes publics. Les technologies de l'information et les télécommunications (TI) ne sont pas seulement la clé pour accomplir efficacement ces activités. Très souvent, elles sont une condition préalable du fonctionnement même des administrations.

Les exigences en matière de fiabilité et de performance sont d'autant plus grandes que les TI sont importantes. Les citoyens et les entreprises attendent des administrations une capacité de réponse qui ne peut plus être assurée sans TI. Et ce qui est vrai en temps normal est encore plus pertinent en cas de catastrophe naturelle ou autre.

Plus l'information est communiquée par voie électronique, plus la question de sa sécurité, de son authenticité et de sa confidentialité est importante. L'accès des services publics et du public à l'information ne contredit pas le besoin de protection de l'information.

L'achèvement du marché intérieur européen a mis en lumière la dimension européenne des points soulevés ci-dessus. La mobilité des personnes, des capitaux, des marchandises et des services implique que la dimension européenne des politiques ne concerne pas seulement «Bruxelles». Au contraire, qu'il s'agisse de sécurité sociale ou de pensions, d'enregistrement d'entreprises ou d'affaires familiales, de sécurité alimentaire ou de contrôle des importations de poissons, les administrations nationales, régionales ou locales impliquées dans ces domaines d'activité agissent en tant qu'administrations européennes. En accomplissant leurs tâches, elles s'appuient sur des échanges d'informations avec leurs homologues dans d'autres parties de l'Union européenne.

Si le service aux citoyens et aux entreprises doit rester, pour l'essentiel, le domaine des administrations nationales, des programmes communautaires comme IDA (Interchange of Data between Administrations) apportent une véritable valeur ajoutée en encourageant l'interopérabilité et donc en permettant la libre circulation de l'information entre administrations. TESTA doit être évalué en fonction de la manière dont il atteint cet objectif.

Cette brochure décrit les services disponibles via TESTA et explique en passant certains des concepts fondamentaux sous-jacents. La section consacrée aux procédures indiquera aux organismes publics intéressés par TESTA quelles démarches pratiques entreprendre ensuite. De manière générale, ce catalogue des services TESTA devrait fournir aux lecteurs des indications utiles sur la manière dont le secteur public européen évolue pour mieux servir les citoyens et les entreprises.

TESTA, Qu'est-ce que c'est?

2

2.1 Programme IDA

IDA (Interchange of Data between Administrations) est un programme communautaire visant à promouvoir l'application des technologies de l'information (IT) dans les échanges d'informations entre les administrations européennes. Il a été adopté par le Conseil de ministres et le Parlement européen et est entré en vigueur en août 1999.

Le programme s'appuie sur deux décisions: 1719/1999/CE et 1720/1999/CE [Réf. 1 et 2].

- La décision 1719/1999/CE définit les principes généraux pour la mise en œuvre de projets télématiques sectoriels à l'appui de politiques communautaires spécifiques.

- La décision 1720/1999/CE appelle la Communauté à assurer une approche technique cohérente et coordonnée des projets télématiques pour garantir l'interopérabilité et l'efficacité.

Parce qu'il rassemble des décideurs et des acteurs nationaux et européens, le programme IDA est à la fois un forum de coordination et un fournisseur de solutions pour les réseaux télématiques.

2.2 TESTA: une approche collaborative

TESTA est le projet IDA visant à fournir des services trans-européens pour la télématique entre administrations (trans-European services for telematics between administrations). Il a été lancé en 1996 et, au début de 2000, il est entré dans sa deuxième phase. Dans la terminologie d'IDA, TESTA est un service *générique*, c'est-à-dire un service qui devrait répondre aux besoins des administrations quel que soit leur domaine d'activité.

TESTA répond au besoin croissant d'échanger des informations entre administrations européennes. Il s'agit de couvrir l'ensemble des États membres et des pays de l'AELE ainsi que, de plus en plus, les pays candidats à l'adhésion. En termes de portée, cela présuppose un degré de capillarité permettant de communiquer avec toute administration impliquée dans la mise en œuvre d'une politique européenne. Cet objectif ambitieux ne peut être atteint qu'en unissant les forces des initiatives nationales et européennes.

L'approche TESTA est «collaborative»: elle s'appuie sur les efforts nationaux pour établir des réseaux administratifs nationaux, régionaux ou locaux en soudant ceux-ci à un réseau trans-européen. IDA fournit l'«EuroDomaine», le réseau reliant les réseaux nationaux/régionaux/locaux et les «EuroGates», les points d'accès, tandis que les administrations nationales prennent en charge la connexion à l'«EuroDomaine».

2.3 Concepts de base

Les concepts de base sur lesquels s'appuie TESTA proviennent des Orientations pour l'architecture IDA (IDA Architecture Guidelines) [Réf. 3]. Ce sont:

- l'«EuroDomaine»;
- le «Domaine local»;
- l'«EuroGate».

L'«EuroDomaine» est défini comme «un ensemble commun de services télématiques paneuropéens approuvé, détenu et géré par la communauté IDA, permettant une liaison transparente entre différents domaines locaux de la communauté européenne des administrations des États membres (y compris les réseaux qui relient des administrations nationales) et des institutions européennes, tels que les appliquent un ou plusieurs fournisseurs de services».

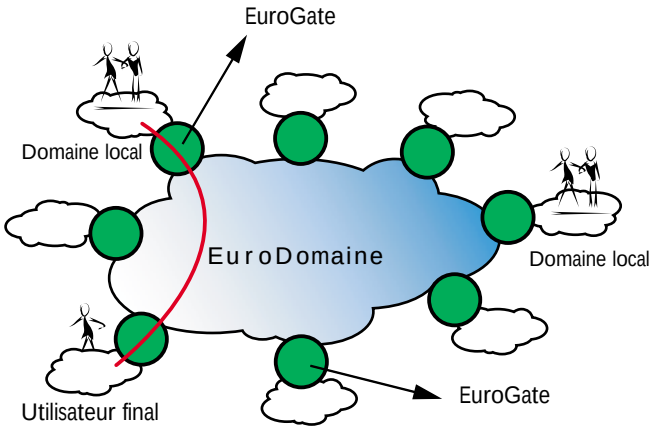
En termes de réseaux, l'«EuroDomaine» peut être vu comme un réseau principal (backbone), défini par les options d'accès, les emplacements des points d'accès et les services fournis entre ceux-ci.

Un «Domaine local» est «un ensemble de services télématiques homogènes utilisés par les administrations nationales (y compris les réseaux reliant des administrations nationales) ou les institutions européennes».

En termes de réseaux, le domaine local peut aller d'un simple réseau local (LAN) à un réseau national qui fait lui-même office de réseau principal (backbone) national.

Les «EuroGates» remplissent un rôle de médiation entre l'«EuroDomaine» et les domaines locaux. «[…] deux «EuroGates» assurent la connexion et l'interopérabilité entre deux domaines locaux quelconques via l'«EuroDomaine» (mais aussi vers les services «EuroDomaine» proprement dits). Ceci permet de maximiser l'indépendance technique entre l'«EuroDomaine» et les «domaines locaux». Un EuroGate peut être décrit comme «un ensemble de services, comprenant à la fois des aspects logiciels et matériels et présentant les fonctions nécessaires de connectivité et d'interopérabilité entre les domaines locaux et l'«EuroDomaine». Il permet également de délimiter les champs de compétence entre les domaines.»

En termes de réseaux, un «EuroGate» peut être considéré comme un routeur donnant directement accès à et géré par l'«EuroDomaine».



2.4 Avantages

TESTA doit être évalué en fonction de la manière dont il répond aux besoins des administrations souhaitant communiquer avec leurs homologues en Europe. Ceci est décrit dans les chapitres suivants. De plus, il existe également des avantages plus généraux à adopter une approche coordonnée de l'échange d'informations entre administrations plutôt que de créer des solutions sur mesure. Ce sont:

- l'obtention d'une interopérabilité non seulement au sein d'un secteur mais également entre différents secteurs administratifs;
- l'obtention d'une interopérabilité entre les États membres et la Communauté;
- la convergence vers une interface télématique commune entre la Communauté et les États membres;
- la rationalisation des opérations, la réduction de la maintenance;
- la mise en œuvre plus rapide de nouveaux projets;
- une sécurité et une fiabilité plus grandes;
- un meilleur rapport coût-efficacité.

Ces objectifs font écho aux préoccupations du Parlement européen et des États membres d'améliorer l'efficacité et la rentabilité dans la mise en œuvre des projets télématiques trans-européens. Ils sont au cœur du programme IDA et TESTA est un exemple pratique de la manière dont ces objectifs se traduisent dans les services opérationnels.

Aperçu du service TESTA 3

3.1 Plate-forme IP

3.1.1 Fonctionnalité

La fonction essentielle de TESTA est de faciliter les communications entre les domaines locaux, qu'il s'agisse de réseaux nationaux ou régionaux ou d'institutions ou agences européennes. À cet effet, IDA fournit un réseau principal (backbone) européen pour les échanges de données administratives, qui fait office de plate-forme d'échange d'informations entre administrations: tout site connecté à l'«EuroDomaine» peut communiquer avec tout autre site connecté de façon similaire.

L'«EuroDomaine» est séparé et protégé de l'Internet public et il présente un certain nombre d'avantages par rapport à celui-ci, à savoir:

- il est spécialisé dans les communications trans-européennes du secteur public et donne accès au plus grand nombre d'administrations européennes de tout réseau privé;

- il opère à des vitesses qui permettent de gérer non seulement les communications «best effort» mais également des applications en temps réel;

- il offre une sécurité accrue du fait qu'il est découplé d'Internet;

- il utilise systématiquement la traduction des adresses réseau à chaque point d'accès, cachant ainsi les structures d'adressage du système local;

- il possède un plan d'adressage IP clair, structuré par entités géographiques et opère sur une série d'adresses spéciales qui ne sont pas «routables» par Internet;

- il possède un routage redondant intégré et il est régi par des garanties de disponibilité; des capacités de surveillance du réseau et d'intervention de sécurité sont en place;

- il permettra la confidentialité de l'information par l'introduction du cryptage et d'autres mesures de protection, tant au niveau du réseau principal (backbone) qu'aux niveaux locaux;

- il peut être renforcé par d'autres services IDA, notamment l'infrastructure à clé publique (PKI) d'IDA et l'outil de support pour groupes de travail (CIRCA) afin d'offrir davantage de sécurité et de services;

- il est régi par des garanties de niveau de service contractuellement contraignantes;

- il dépend d'une seule autorité contractuelle: IDA.

3.1.2 Emplacements des «EuroGates»

Pour simplifier l'accès à l'«EuroDomaine», un certain nombre de points d'accès, les «EuroGates» sont définis dans chaque pays. Ces «EuroGates» offrent plusieurs méthodes de connexion et sont eux-mêmes interconnectés via un réseau à haute capacité et haute disponibilité. Les «EuroGates» et l'«EuroDomaine» sont gérés par Global One. Les «EuroGates» correspondent généralement aux points de présence IPVPN de Global One, qui sont énumérés par pays ci-dessous. De plus, il est possible d'accéder à l'«EuroDomaine» par toute autre implantation Global One; une liste peut être fournie sur demande.

Pays	Emplacements des «EuroGates»
Union européenne	
Belgique	Bruxelles
Danemark	Copenhague
Allemagne	Francfort
	Hambourg
	Dusseldorf
	Stuttgart
	Munich
Grèce	Athènes
Espagne	Madrid
	Barcelone
France	Couverture nationale complète (ossature France Telecom)
Irlande	Dublin
Italie	Milan
	Rome
Luxembourg	Luxembourg
Pays-Bas	Amsterdam
Autriche	Vienne
Portugal	Lisbonne
Finlande	Helsinki
Suède	Stockholm
	Göteborg
	Malmö
	Sundsvall
	Orebro
Royaume-Uni	Londres
	Archway
	Birmingham
	Manchester
	Milton Keynes

Pays candidats	
Estonie	Tallinn
République tchèque	Prague
Slovaquie	Bratislava
Hongrie	Budapest
Roumanie	Bucarest
Bulgarie	Sofia
Lettonie	Riga
Pologne	Bydgoszcz
	Gdansk
	Katowice
	Cracovie
	Poznan
	Varsovie
	Wroclaw

Pays candidats	
Lituanie	Pas encore de présence
Slovénie	Pas encore de présence
Chypre	Pas encore de présence
Malte	Pas encore de présence
Turquie	Istanbul

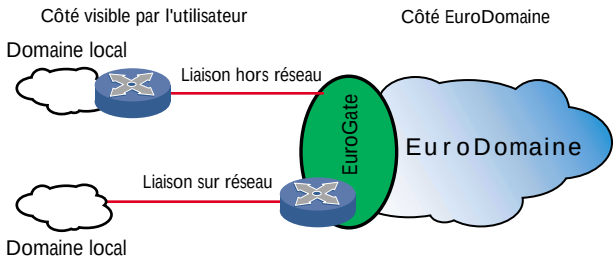
Autres	
Islande	Reyjkjavik
Norvège	Oslo
Suisse	Zurich
	Genève

3.1.3 Accéder aux «EuroGates»

3.1.3.1 Accès sur réseau et hors réseau

Chaque «EuroGate» supporte deux types d'accès permanent: «sur réseau» et «hors réseau». Les connexions «sur réseau» sont établies lorsque le fournisseur de réseau du domaine local assume la responsabilité de la connexion WAN entre son routeur périphérique et l'«EuroGate». Pour un meilleur contrôle sur cette liaison, le fournisseur de domaine local peut souhaiter terminer la liaison WAN avec un routeur dans les installations de l'«EuroGate».

Les connexions sont dites «hors réseau» lorsque le fournisseur de l'«EuroDomaine» est responsable de la connexion WAN depuis l'«EuroGate» jusqu'au point d'accès du fournisseur local (ou de l'administration locale). Dans ce cas, la liaison sera terminée par un routeur de l'«EuroDomaine» situé dans les installations du domaine local.



3.1.3.2 Protocoles d'accès

Les «EuroGates» sont accessibles au moyen de tout protocole moderne: notamment lignes louées (IP natif), relais de trames ou ATM. Sur les sites connectés hors réseau, l'interface client sera un port LAN sur le routeur fourni par l'opérateur de l'«EuroDomaine».

3.1.3.3 Accès commuté (dial-up)

Un accès commuté à l'«EuroDomaine» par RTC ou RNIS peut être établi. Ce service est intéressant pour les administrations qui ont un besoin limité ou occasionnel de communiquer via TESTA et pour les personnes qui ont besoin d'un accès mobile. Les utilisateurs sont identifiés par des serveurs RADIUS via des identificateurs d'accès réseau (NAI) et des mots de passe et sont ensuite acheminés vers les adresses réseau pour lesquelles ils ont des droits d'accès.

3.1.3.4 Vitesses d'accès

Un accès permanent aux «EuroGates» peut être commandé à des vitesses allant de 64 Kbps à 34 Mbps. Des services commutés sont disponibles jusqu'à 56 Kbps pour les services analogiques (RTC) et jusqu'à 64 Kbps pour l'accès commuté numérique (RNIS).

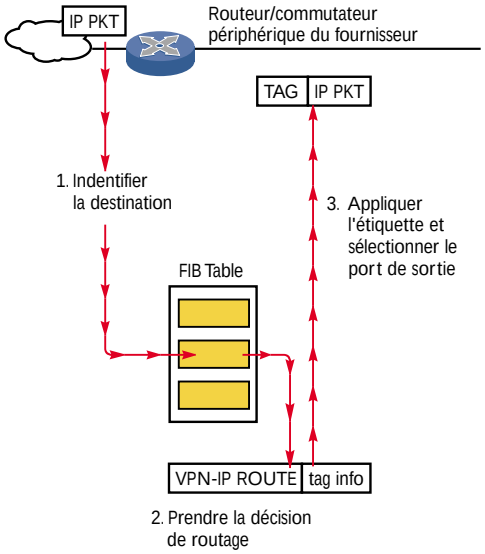
3.1.4 Technologie «EuroDomaine»

Les services «EuroDomaine», qui sont exploités par Global One, sont basés sur son produit Global IP VPN. Celui-ci offre des services Intranet et Extranet spécialisés utilisant les protocoles normalisés TCP/IP (Transmission Control Protocol/Internet Protocol) pour transférer des informations entre points de présence (POP). Il utilise l'infrastructure de base ATM NGEN (Next Generation) sous-jacente de Global One pour les services de transport.

Global IP VPN a été mis en œuvre en utilisant la technologie «tag switching» (commutation par étiquettes) qui évoluera pour soutenir la norme MPLS (Multi-Protocol Label Switching) de l'IETF (Internet Engineering Task Force).

La technologie MPLS normalisée et approuvée par l'IETF accélère le flux du trafic sur le réseau en évitant l'analyse des paquets par des routeurs intermédiaires (hops). Cela se fait au moyen d'étiquettes qui sont attachées au paquet par les routeurs périphériques du réseau principal (backbone), sur la base d'informations stockées dans la base d'information de transmission (FIB).

Les étiquettes sont également utilisées pour mettre en œuvre des réseaux privés virtuels (VPN).



La technologie MPLS combine les avantages du routage de couche 3 avec les avantages de la commutation de couche 2. Comme les adresses IP ne sont pas évaluées durant le transit par le réseau principal (backbone), MPLS n'impose aucune limitation d'adressage IP.

3.1.5 Structure des adresses de l'«EuroDomaine»

Les domaines locaux sont interconnectés via l'«EuroDomaine», au moyen d'adresses IP enregistrées TESTA II. Les adresses sont indépendantes du fournisseur mais elles sont gérées par l'opérateur de l'«EuroDomaine», Global One. Pour chaque domaine local, le point d'entrée à TESTA II est configuré avec le support de la traduction des adresses réseau (NAT) traduisant les adresses IP internes du domaine local en adresses IP enregistrées TESTA II.

Le bloc d'adresses 62 62 0 0/17 a été alloué par l'*European IP registration* authority (RIPE) à TESTA II. Une partie de cette série a été réservée pour une utilisation ultérieure (notamment pour les pays candidats). En général, l'allocation des adresses sera régie par la géographie, chaque pays recevant une série d'adresses de classe C. Les institutions européennes feront exception à cette règle: elles recevront des blocs d'adresses d'une partie distincte de la série ci-dessus.

L'allocation d'espace d'adressage concerne uniquement les communications via l'«EuroDomaine» (pas les communications internes au domaine local). Le support NAT dynamique (ou Port Address Translation) sera utilisé autant que possible (de manière à réduire le nombre d'adresses IP enregistrées TESTA II nécessaires).

3.1.6 Convention pour les noms «EuroDomaine»

Des noms de domaine sont utilisés pour l'adressage d'ordinateurs et d'utilisateurs via les réseaux IP. Les ressources d'information qui doivent être rendues accessibles via TESTA seront adressées en utilisant la convention TESTA pour les noms de domaine. Il a été convenu d'adopter le système suivant, qui permet de faire la distinction entre les ressources accessibles par Internet et accessibles par TESTA.

<3ème niveau>.eu-admin.net où *«3ème niveau»* pourrait être un dénominateur de pays ou une organisation ou autre, *eu-admin.net* est le domaine de niveau supérieur.

En dessous du domaine de niveau supérieur eu-admin.net, des descripteurs organisationnels (www.portal.de.eu-admin.net) ou basés sur des projets (eudra.eu-admin.net) peuvent être insérés.

Pour éviter les conflits au niveau des noms et assurer un routage correct, toutes les ressources d'information qui doivent être accessibles via TESTA doivent être enregistrées auprès des responsables du réseau «EuroDomaine».

3.2 Configurations de recouvrement

3.2.1 Classes de trafic

L'«EuroDomaine» garantit de multiples niveaux de service, permettant au réseau principal (backbone) de gérer les priorités entre différents types de trafic. La différenciation de la classe de service s'effectue sur la base du champ de préséance à 3 bits dans l'en-tête IP.

Plusieurs mécanismes sont mis en œuvre afin de supporter des niveaux de service de bout en bout (retard, abandons de paquet) sur le réseau. Ces mécanismes sont le contrôle d'admission (CAR - Committed Access Rate), la gestion de la congestion (WRED - Weighted Random Early Detection) et la gestion de la queue (Weighte Fair Queuing).

Le mécanisme CAR classe les paquets entrants (fixe/modifie la préséance IP) et gère la bande passante d'accès par la gestion du débit. La gestion du débit est mise en œuvre au moyen d'un système «token bucket»: des jetons (token) sont ajoutés dans le seau (bucket) à la vitesse convenue et le nombre de jetons dans le seau est limité par la vitesse normale du port. Les paquets arrivant avec suffisamment de jetons dans le seau sont déclarés conformes (appliquer action conforme), les paquets arrivant avec insuffisamment de jetons dans le sceau sont déclarés en excès (appliquer action d'excès). Les actions d'excès peuvent être, par exemple, un abandon du paquet (packet drop) ou une modification de la préséance IP du paquet. Les actions à appliquer au paquet en excès sont configurées par Global One.

Avec le mécanisme WRED, le routeur surveille la taille moyenne de la queue. Lorsque la congestion est imminente, il notifie de façon aléatoire à plusieurs connexions de réduire la vitesse de transmission. La notification se fait en utilisant des abandons de paquet (packet drops), ce qui constitue un signal explicite au TCP de ralentir la transmission. WRED combine RED avec la préséance IP pour mettre en œuvre de multiples classes de service. Dans les réseaux congestionnés, le trafic de classe inférieure est ralenti en premier, avant le trafic de classe supérieure. Cette stratégie entraîne moins d'abandons de paquets et davantage de bande passante disponible pour le trafic de classe supérieure.

Weighted Fair Queuing est un algorithme de programmation des paquets utilisé pour déterminer l'ordre dans lequel les paquets sont envoyés à la liaison de transmission. Global IP VPN utilise la méthode CB-WFQ (Class-Based Weighted Fair Queuing). Avec cette méthode, les paquets sont classés dans 4 queues fondées sur les 2 bits les moins significatifs de la préséance IP du paquet. Chaque queue est pondérée. Les queues en attente sont servies en proportion de leur poids. Le poids détermine la quantité de bande passante que chaque queue active est autorisée à consommer pendant les périodes de congestion. L'opérateur du réseau configure les pourcentages des différentes queues.

Sur l'«EuroDomaine», des mécanismes de régulation du trafic aux points d'accès et l'étiquetage des paquets sur le réseau principal (backbone) sont combinés pour fournir trois classes de trafic: «Exclusive», «Business» et «Economy». Les paquets IP sont traités en fonction de celle des trois classes à laquelle ils sont alloués, sur la base des adresses IP ou de l'application (numéro de port).

3.2.2 Réseaux virtuels privés

L'«EuroDomaine» supporte la technique Tag-VPN (Tag Switching for Virtual Private Networks) Celle-ci repose sur le concept de «label swapping»: les petites unités de données contiennent une étiquette de longueur fixe qui indique aux dispositifs du réseau comment traiter l'information. Les Tag-VPN assurent une connectivité *«any-to-any»*; ils se déploient également facilement et économiquement pour supporter de nouveaux utilisateurs.

3.3 Services d'application TESTA

3.3.1 Services de noms de domaine

Les services de noms de domaine relient des localisateurs de ressources tels que www.eu-admin.net à des adresses IP et les rendent accessibles via le réseau.Toutes les ressources accessibles via TESTA sont clairement identifiées par un domaine de niveau supérieur spécifique (eu-admin. net).

Un serveur de noms de domaine central est exploité et maintenu au niveau de l'«EuroDomaine»; il contient des informations sur toutes les ressources auxquelles il donne accès. En raison de l'utilisation de la traduction des adresses réseau (NAT) à chaque accès à l'«EuroDomaine», l'adresse IP réelle d'un serveur spécifique dans un domaine local reste cachée et est traduite en une série IP de la série TESTA.

Un document décrit comment les domaines locaux doivent configurer l'accès au serveur central des noms de domaine et comment enregistrer des sites d'information sur l'«EuroDomaine» [Réf. 5].

3.3.2 Relais de courrier électronique

Le courrier électronique peut être routé comme n'importe quel autre trafic de données sur le réseau «EuroDomaine» mais TESTA fournit un certain nombre de services à valeur ajoutée via son relais de courrier électronique. En plus d'héberger des boîtes à lettres électroniques spécifiques à TESTA, l'infrastructure peut mettre en œuvre des listes de distribution de courrier et des politiques de routage. Cela permet de l'utiliser comme une chambre de compensation pour les messages adressés aux administrations connectées à l'«EuroDomaine». Des mécanismes anti-virus peuvent également être mis en place.

Le relais de courrier électronique TESTA s'appuie sur une plate-forme matérielle à grande disponibilité située au niveau des fonctionnalités d'application centrales de TESTA et il est protégé par un pare-feu. Un document décrit comment demander et utiliser ses possibilités [Réf. 7].

3.3.3 Passerelle d'information

Que le travail concerne la sécurité sociale, l'emploi, l'agriculture ou tout autre domaine, avoir accès à l'information est un élément essentiel du service public. Cependant, rechercher l'information, ne serait-ce que la trouver, est souvent difficile.

Pour faciliter la navigation vers les ressources d'information accessibles via l'«EuroDomaine», TESTA offre une passerelle d'information qui consolidera et maintiendra l'information indiquant où et comment accéder aux données relatives à des domaines spécifiques, qu'elles soient situées au niveau européen ou dans un des domaines connectés.

Cette fonctionnalité est accessible au moyen d'un outil de navigation et fournira un accès indexé aux sites présentant un intérêt spécifique. En tant que fonctionnalité d'échange centrale, elle offre une fonction de tableau noir permettant à ceux que cela intéresse d'annoncer des manifestations ou des publications à d'autres administrations ou de rechercher des partenaires dans des projets. En tant que site web central de TESTA, elle fournit également des informations en ligne sur le réseau et son utilisation ainsi que de la documentation supplémentaire et des points de contact.

Elle est accessible via l'URL www.eu-admin.net. Un document décrit comment les fournisseurs de contenu peuvent l'utiliser pour créer des liens vers leurs sites d'information [Réf. 9].

3.3.4 Hébergement

Si des projets transeuropéens souhaitent exécuter des applications accessibles aux administrations européennes, l'infrastructure d'hébergement web de TESTA peut fournir une plate-forme matérielle spéciale complète avec des liens redondants à TESTA.

Cette infrastructure n'est pas liée à Internet et elle est protégée par un pare-feu. Elle permet le contrôle des accès au site, la protection incendie et l'alimentation de secours. L'allocation des adresses IP est effectuée par Global One, qui exploite également le serveur de noms de domaine pour supporter jusqu'à trois domaines par client.

Un document décrit comment les fournisseurs de contenu peuvent faire usage de cette fonction [Réf. 11].

3.4 Services d'information locaux

3.4.1 Services de localisation

Les services des noms de domaine (DNS) de TESTA résoudront les localisateurs de ressources en adresses IP et masqueront les aspects d'adressage à l'utilisateur et aux applications. Cela présuppose que l'utilisateur connaisse un site d'information spécifique auquel il veut accéder. Souvent, cependant, cette connaissance n'est pas disponible et les utilisateurs sont confrontés moins à la difficulté du routage du réseau qu'à l'absence d'une vue d'ensemble sur les ressources disponibles via le réseau. Pour résoudre ce problème, TESTA exploite une passerelle d'information standard qui énumérera les sites d'intérêt, qu'ils soient situés sur l'«EuroDomaine» ou dans un domaine local. En outre, plusieurs domaines connectés mettent en place des portiques nationaux pour canaliser l'accès à l'information administrative. Si nécessaire, la passerelle d'information TESTA fera le lien avec ceux-ci.

3.4.2 Gestion des droits d'accès

La capacité d'un utilisateur d'accéder à une source d'information locale via TESTA est influencée par trois facteurs:

- les restrictions du trafic imposées par l'«EuroDomaine»;
- les restrictions imposées par le domaine local ou distant;
- les restrictions imposées par l'application.

TESTA ne limite pas l'accès entre les domaines locaux et l'«EuroDomaine», à moins que cela ne soit explicitement demandé et justifié par une communauté d'utilisateurs particulière. Dans les domaines locaux, les politiques de contrôle d'accès au réseau différeront d'un domaine à l'autre et l'accès pourra être restreint non seulement pour les utilisateurs souhaitant entrer dans le domaine local pour accéder à un site d'information spécifique mais également pour les utilisateurs de l'intérieur du domaine local souhaitant en sortir pour atteindre un site dans un domaine distant.

En général, cependant, des restrictions d'accès seront mises en place par application sur les sites d'information. La gestion des droits d'accès au niveau de l'application est basée sur le concept de «propriété» de l'information. Lorsque l'information est restreinte, le droit d'accorder ou de retirer l'accès appartient au propriétaire de l'information et cette personne définira la procédure par laquelle les droits d'accès sont gérés.

La passerelle d'information TESTA centrale fournira des informations non seulement sur la manière de localiser des sites d'information mais également sur la personne à contacter pour demander l'accès à ceux-ci.

3.5 Services de support

Les heures de support standard pour les utilisateurs TESTA sont 24 heures sur 24, 7 jours sur 7. Le support des services «EuroDomaine» est assuré par Global One via ses dispositifs de support standard. Ses centres de support peuvent être contactés via des numéros de téléphone gratuits dans toute l'Union européenne et dans les 11 langues de l'Union européenne.

Un support supplémentaire est assuré par le gestionnaire de service assigné par Global One aux clients TESTA. Des informations plus complètes sur l'organisation du support peuvent être trouvées dans [Réf.10], disponible sur demande.

Comme TESTA opère sur le réseau principal (backbone) de l'«EuroDomaine», le support de service sera assuré à différents niveaux. Le premier point de contact pour les utilisateurs des administrations nationales ou locales sera typiquement leurs dispositifs d'assistance respectifs. Une infrastructure de support supplémentaire peut être mise en place par application, et IDA peut assurer un suivi centralisé de la résolution de problèmes complexes via son projet ASSIST [Réf. 8].

3.6 Garanties de niveau de service

Les niveaux de service sont garantis par contrat et des pénalités sont prévues. Ce qui suit est un extrait des garanties s'appliquant aux services TESTA. Le texte intégral de l'accord de niveau de service (SLA — Service Level Agreement), qui inclut également les pénalités, peut être obtenu sur demande.

3.6.1 Disponibilité

La disponibilité minimale des services est la suivante:

Éléments de service	Disponibilité minimale
Services «EuroGate» à tout endroit	99,7 % mensuellement 99,9 % annuellement
Accès sur réseau à un «EuroGate»	99,7 % mensuellement 99,9 % annuellement
Accès hors réseau à un «EuroGate»	99,7 % mensuellement avec sauvegarde
Plate-forme de site web	99,5 % mensuellement
Service pare-feu	99,5 % mensuellement
Services cryptographiques	99,7 % mensuellement

Le contractant peut employer des solutions de sauvegarde pour atteindre les valeurs convenues.

Les garanties de disponibilité ne couvrent pas les interventions de maintenance planifiées. Toutes les interventions de maintenance planifiées seront entreprises en dehors des heures de travail normales, dans une fenêtre de maintenance, le samedi de 2 h à 10 h du matin (fuseau horaire de l'Europe occidentale).

3.6.2 Délai de rétablissement

Les délais maxima pour le rétablissement des services sont les suivants:

Description des défaillances	TTR	MTTR
Défaillance(s) interdisant l'accès à un ou plusieurs «EuroGates» à partir d'un domaine local.	2 heures	2 heures
Défaillance(s) réduisant la qualité de service d'un «EuroGate» particulier à un ou plusieurs autres «EuroGate».	6 heures	4 heures
Défaillance(s) affectant l'offre de services web.	6 heures pendant le service	4 heures
Défaillance(s) affectant l'offre de services pare-feu.	4 heures	4 heures
Défaillance(s) affectant l'offre de services cryptographiques.	6 heures	4 heures

Le contractant peut employer des solutions de sauvegarde pour atteindre les valeurs convenues.

3.6.3 Retard du réseau

Liaison au réseau et classe de service	Retard maximum aller-retour
«EuroGate» à «EuroGate» classe de service «Exclusive»	200 ms
«EuroGate» à «EuroGate» classe de service «Business»	250 ms
«EuroGate» à «EuroGate» classe de service «Economy»	400 ms
Accès hors réseau à l'«EuroGate» le plus proche	[Voir note ci-dessous.]

Note: *Les valeurs maximales aller-retour énumérées ci-dessus concernent les connexions «EuroGate» à «EuroGate» sans filtrage spécifique basé sur des contrôles des droits d'accès par la plate-forme de gestion «EuroDomaine». Elles n'incluent pas non plus le temps de cryptage, de conversion du protocole, etc.*

Les mesures du retard du réseau sont effectuées toutes les 60 minutes durant les heures de service pour les connexions «EuroGate» à «EuroGate» et toutes les 60 minutes durant les heures de service pour les connexions hors-réseau à «EuroGate».

3.6.4 Rapports

Paramètres	Couverture
Disponibilité pendant les heures de service et de support	- Par «EuroGate» - Par accès hors réseau à l'«EuroGate» - Par accès sur réseau à l'«EuroGate»
Volume total (Mbytes) durant les heures de service	- Par EuroGate, entrant de et sortant vers l'«EuroDomaine» - Par interface «EuroGate», entrant des domaines locaux
Consommation moyenne/ en pointe de la bande passante durant les heures de service.	- Entre les interfaces «EuroDomaine» de tous les «EuroGates».
Retards du réseau durant les heures de service	

Les informations des rapports seront communiquées par courrier électronique ou remises en main propre lors de la réunion mensuelle de suivi ainsi qu'en ligne, via une interface web. Elles seront communiquées dans les dix jours ouvrables après la fin du mois précédent.

3.6.5 Helpdesk

Phase de traitement	Retour d'information	Délai
Rapport de problème	Confirmation et numéro d'enregistrement	1 heure
Analyse et résolution du problème	2 heures	
Clôture de l'incident	2 heures	

3.7 Sécurité

3.7.1 Niveaux de sécurité

Comme TESTA est un réseau de réseaux, composé du réseau principal «EuroDomaine» et de réseaux du domaine local, la sécurité doit être mise en œuvre à plusieurs niveaux: sur le réseau principal, sur les réseaux du domaine local et sur le site de l'utilisateur final. Chacune des administrations participantes aura soin de mettre en œuvre des niveaux de sécurité adéquats dans l'infrastructure de réseau sous son contrôle.

3.7.2 Sécurité assurée par TESTA

TESTA met en place un certain nombre de mesures qui renforceront la sécurité du réseau principal «EuroDomaine». Celles-ci abordent les dimensions disponibilité et confidentialité de la sécurité, tandis que l'authentification et l'autorisation sont traitées au niveau de l'application.

La disponibilité du réseau et l'accès aux ressources en informations constituent une exigence de sécurité essentielle de tous les réseaux. C'est pourquoi TESTA s'appuie sur les garanties de disponibilité les plus élevées actuellement offertes par le marché. Ces garanties s'appliquent non seulement aux composantes du réseau mais également aux services de support tout aussi importants que sont le DNS et le relais de courrier électronique.

Le réseau est construit spécifiquement pour des administrations et il est complètement séparé d'Internet, ce qui élimine les menaces pour la sécurité qui pourraient en résulter. En outre, l'utilisation cohérente de la traduction d'adresse à chaque point d'accès contribue à protéger les domaines locaux si la sécurité de l'«EuroDomaine» devait être compromise. La surveillance permanente des éléments essentiels du réseau et un contrôle de gestion clairement identifié sur l'«EuroDomaine» et les réseaux connectés facilitent l'intervention en cas d'incidents relatifs à la sécurité.

TESTA protège les informations voyageant à travers l'«EuroDomaine» contre les accès non autorisés. Sur le plan physique, cela comprend des mesures visant à contrôler l'accès aux composants du réseau, exploités par Global One. Cela inclut également l'utilisation étendue de fibre optique, l'un des supports de transmission les plus sûrs.

Sur le plan logique, la confidentialité est renforcée par l'introduction de dispositifs de cryptage aux principaux points d'accès de l'«EuroDomaine». Ces dispositifs permettent le cryptage hardware des paquets IP en ITSEC niveau 3 en utilisant des algorithmes de cryptage tels que Alternating DES (112 bits), IDEA (128 bits), 3-DES (112 ou 168 bits). La gestion des dispositifs de cryptage est assurée par Global One, tandis que la gestion des clés restera de la responsabilité de la Commission.

3.7.3 IDA PKI

Le projet IDA PKI (IDA Public Key Infrastructure for Closed User Groups) offre une solution de sécurisation efficace, normalisée, de bout en bout, mise en œuvre sur la couche d'application. Le projet a été lancé au début de 1999 dans le but de mettre en place une autorité de certification (Certification Authority — CA) accessible à toutes les administrations des États membres. Les services IDA PKI sont accessibles via TESTA.

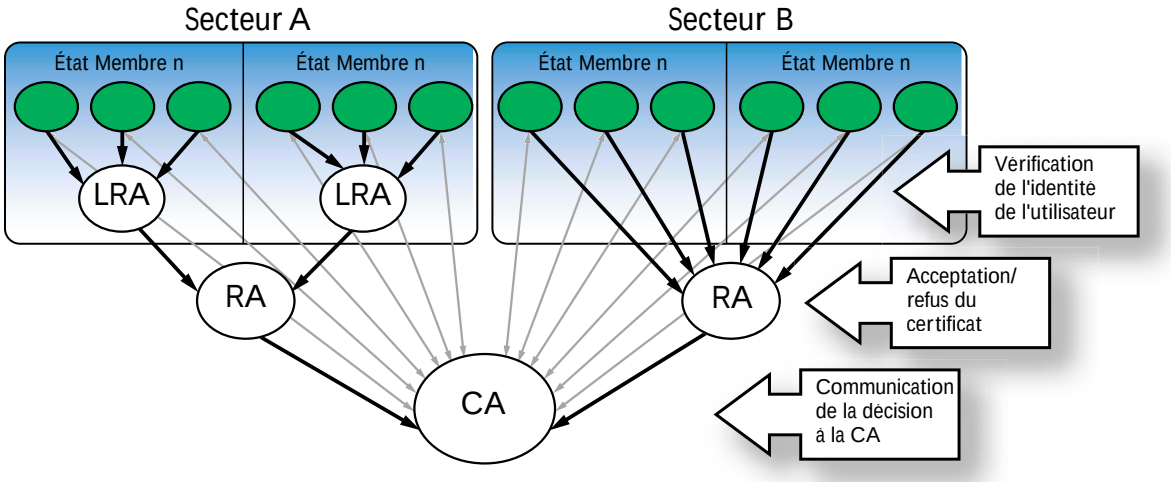
Le projet IDA PKI peut fournir tous les services nécessaires pour la gestion des certificats électroniques (création, révocation, renouvellement) lorsqu'aucune autorité de certification (CA) nationale n'existe ou lorsque, pour une raison quelconque, les utilisateurs ne souhaitent pas utiliser les services de l'autorité de certification nationale. Il devrait compléter et interagir avec les infrastructures mises en place par les États membres, les institutions européennes et la Commission européenne et être capable d'harmoniser la reconnaissance mutuelle des certifications délivrés par ces infrastructures.

Pour autant que l'environnement requis soit mis en place, une infrastructure PKI est essentiellement une organisation; elle s'appuie sur un ensemble de rôles et responsabilités et de procédures que chaque partenaire doit respecter minutieusement et qui sont résumées dan un «Certificate Practice Statement (CPS). La confiance que les utilisateurs peuvent avoir dans l'infrastructure PKI dépend de ces procédures. Elles sont donc essentielles.

Les rôles requis pour mettre en œuvre la sécurité au sein d'un réseau IDA au moyen de certificats à clé publique sont:

- les *utilisateurs finals* qui émettent une demande de certificat, participent à sa création et le révoquent si nécessaire;
- *l'autorité d'enregistrement* (Registration Authority — RA), éventuellement assistée d'une *autorité d'enregistrement locale* (LRA — pour évaluer l'authenticité et la légitimité des demandes;
- *l'autorité de certification* (Certification Authority — CA) pour gérer le cycle de vie des certificats.

Le schéma suivant donne un aperçu général des relations entre les acteurs. Les flèches grasses montrent la circulation de l'information pour émettre un certificat. Les flèches maigres montrent la répartition des certificats.



Les procédures concernées sont détaillées dans les *Certification Practice Statements* (CPS).

La logique des interactions entre ces acteurs peut être décrite comme suit:

1. le candidat détenteur de certificat se connecte au serveur CA et émet une demande pour obtenir un certificat;
2. la RA et le demandeur échangent les informations nécessaires pour vérifier l'identité de l'utilisateur et la légitimité de la demande de certificat; facultativement, une autorité d'enregistrement locale (LRA) est appelée pour témoigner que le demandeur est effectivement habilité à recevoir un certificat;
3. sur la base des résultats de la deuxième étape, la RA approuve ou rejette la demande et enregistre sa réponse sur le serveur CA;
4. si la RA a approuvé la demande à la troisième étape, la CA crée le certificat public du détenteur de certificat et indique à celui-ci où et comment il peut l'obtenir (généralement en le téléchargeant du serveur de la CA);
5. les tiers accordant crédit téléchargent les certificats à clé publique du répertoire de la CA en fonction de leurs besoins.

Des renseignements supplémentaires sur le projet IDA PKI et sur la manière dont il peut être utilisé sont fournis dans [Réf. 12].

Comment demander les services TESTA

4

4.1 Éligibilité

TESTA est un service générique fourni dans le cadre du programme IDA. L'éligibilité pour les services TESTA est régie par les décisions IDA, décrivant les activités communautaires dans le domaine des réseaux télématiques transeuropéens pour les administrations.

TESTA est un réseau administratif européen. Les bénéficiaires potentiels sont:

- les administrations publiques nationales ou européennes (y compris les institutions et agences européennes)
- tout autre organisme public national, régional ou local et
- toute organisation internationale

échangeant ou susceptibles d'échanger des données avec d'autres administrations publiques dans le cadre de la mise en œuvre d'un ou de plusieurs actes communautaires visés aux articles 249 à 256 du Traité établissant la Communauté européenne.

4.2 Procédure

La procédure pour demander les services est simple. Les parties intéressées doivent informer l'unité IDA de leur intérêt en indiquant quels sites exigent l'accès à TESTA et avec qui elles veulent communiquer ainsi que le type de service demandé. Des informations concernant la base juridique de leur communication devraient également être fournies afin qu'IDA puisse vérifier l'éligibilité.

Les demandes de connexion proviendront généralement d'une communauté d'administrations engagée dans un domaine d'activité particulier.

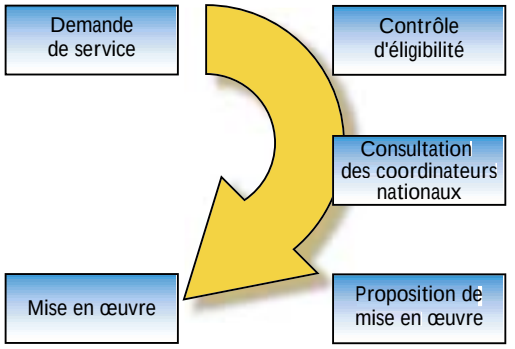
Les demandes de connexion d'administrations individuelles devraient être justifiées en termes de besoin pour les activités de ces administrations.

Les informations suivantes devraient être fournies:

- liste des administrations (nom, lieu, coordonnées des contacts locaux) qui souhaitent être connectées;
- description des services qui sont demandés;
- description succincte des besoins de communication;
- acte juridique ou autre base relative aux besoins de communication;
- lorsqu'une demande est soumise pour le compte d'autres, preuve de l'intérêt des autres administrations (par exemple: compte rendu d'une réunion au cours de laquelle cela a été décidé);
- nom du coordinateur du projet.

Sur la base de ces informations, IDA vérifiera l'éligibilité puis consultera les coordinateurs de réseau nationaux concernant les options de mise en œuvre. À moins qu'une justification raisonnable soit fournie, la préférence sera accordée à l'établissement des connexions via les réseaux administratifs nationaux. Dans des circonstances exceptionnelles, des liens directs à TESTA peuvent être fournis mais sous réserve des limites de financement décrites dans le chapitre sur le partage des coûts.

Une fois que les coordinateurs nationaux ont été consultés, le coordinateur de projet recevra une proposition de mise en œuvre pour approbation. Si toutes les infor-mations requises sont soumises dans la demande de service, une proposition de mise en œuvre peut généralement être soumise dans un délai de 4-6 semaines.



4.3 Assistance

Les administrations, ou communautés d'administrations, qui ont besoin d'échanger des données mais souhaitent obtenir une assistance pour formuler leurs besoins peuvent faire usage des services du projet ASSIST.

Le but de ASSIST est de fournir un support pré-opérationnel et opérationnel aux utilisateurs de TESTA et aux utilisateurs potentiels sur la base d'un contrat cadre signé avec Unisys (sous-contractant: Aethis Ubizen).

Lorsqu'une assistance est requise pour analyser les besoins en communication, une procédure en deux étapes est suivie.

- Dans une phase de pré-analyse de max. 5 jours, ASSIST interroge le coordinateur de projet afin d'être en mesure d'évaluer la charge de travail et les contraintes de temps de la deuxième étape, l'analyse elle-même. L'équipe ASSIST rend compte à IDA, qui donne alors le feu vert pour la deuxième étape.

- Pendant la phase d'analyse, l'équipe ASSIST étudie les besoins en communication dans une perspective technique et professionnelle afin de mieux comprendre quels flux de données avec quels volumes doivent être supportés et d'aborder des questions telles que la sécurité. Des visites sur site peuvent également être effectuées afin d'examiner l'infrastructure technique existante. Le résultat de cette activité sera typiquement un rapport de recommandations.

L'assistance du type décrit peut être obtenue sur simple demande en indiquant:

- l'acte juridique ou autre base relative aux besoins de communication;
- la liste des administrations (nom, lieu, coordonnées des contacts locaux) à étudier;
- le nom du coordinateur du projet.

Les études de pré-analyse peuvent être généralement réalisées dans un délai de 4-6 semaines à compter de la réception d'une demande d'intervention mais la disponibilité du personnel ASSIST pourrait imposer un délai plus long.

4.4 Coordination avec les initiatives nationales en matière de réseaux

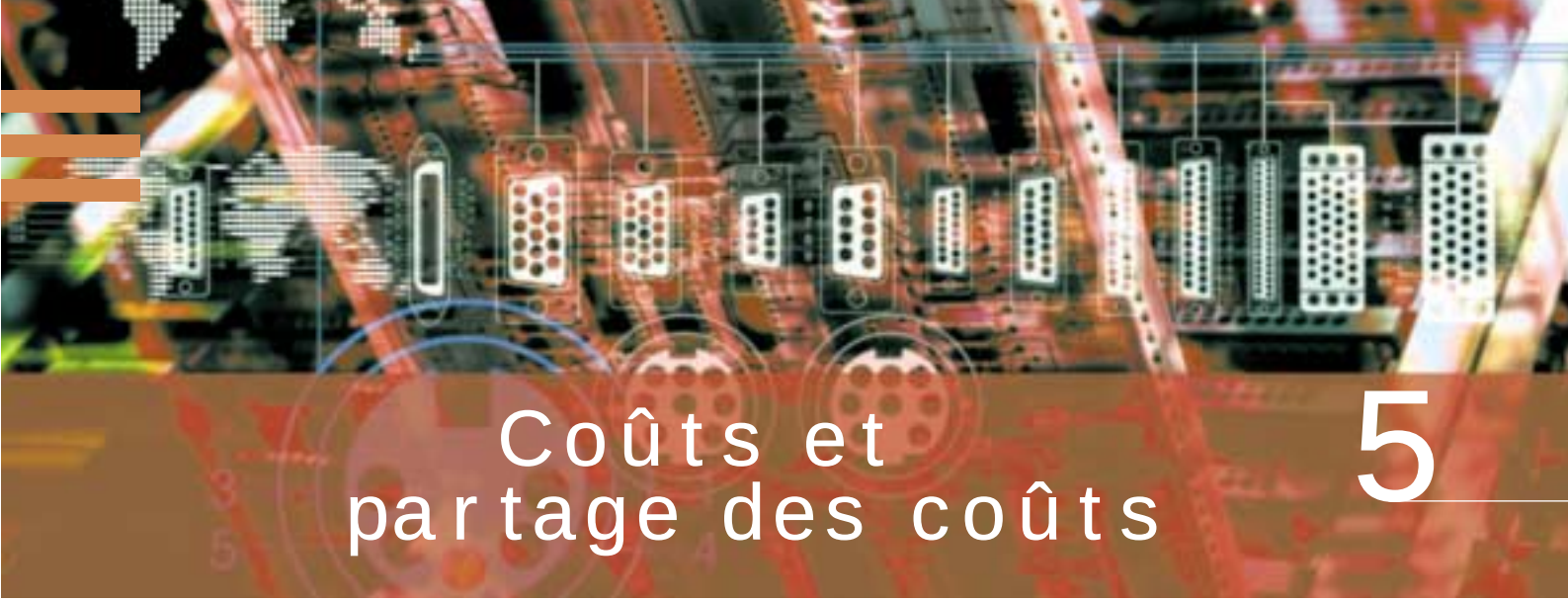
TESTA interconnecte des réseaux administratifs nationaux. Les politiques en matière de réseau, y compris des aspects tels que:

- l'adressage IP
- les noms de domaine
- la sécurité
- les niveaux de service

sont définies en accord avec les coordinateurs des réseaux nationaux.

Les demandes de services TESTA émanant d'une administration nationale sont généralement transmises au coordinateur de réseau national concerné. Dans de nombreux pays, les politiques nationales s'appliquent aux liaisons de télécommunication avec les administrations et les décisions de mise en œuvre de TESTA sont donc prises après consultation du coordinateur national. Deux choix fondamentaux s'appliquent:

- une connexion directe du site concerné à l'«EuroGate» le plus proche;
- une connexion au réseau administratif national, qui est à son tour connecté à un «EuroGate».



Coûts et partage des coûts

5

5.1 Coûts

La liste suivante met l'accent sur les coûts relatifs au réseau de l'établissement d'une connexion à TESTA. Dans certaines circonstances, la connexion à l'«EuroDomaine» peut entraîner des frais administratifs et de gestion et requérir également l'installation d'équipements supplémentaires au niveau local (par exemple: des pare-feux).

Les coûts directs d'une connexion à TESTA couvrent:

- les coûts de la boucle locale (ligne louée ou commutation RTC/RNIS);
- les coûts du routeur ou modem;
- le coût de l'équipement de sauvegarde — si nécessaire;
- les frais de service du fournisseur (surveillance).

Les coûts de la boucle locale varient beaucoup en Europe et, dans certains pays, ils constituent l'élément de coût le plus important. Ils dépendent également de la situation d'un site spécifique et de la distance entre ce site et l'«EuroGate» le plus proche. Pour ces raisons, il est difficile de fournir des estimations. Les ordres de grandeur suivants sont fournis à titre indicatif:

Vitesse	Type d'accès	Coûts mensuels moyens en euro
64	RNIS	395 (1)
64	Ligne louée	1 100 (2) (3)
128	Ligne louée	1 500 (2) (3)

(1) Comprend NAI + routeur + surveillance
(2) Comprend boucle locale + routeur + sauvegarde + surveillance
(3) Coûts d'installation moyens = 2360 euro.

5.2 Partage des coûts

Les règles générales de partage des coûts suivantes s'appliquent aux services fournis dans le cadre de TESTA.

- Les services du réseau principal (backbone) TESTA II (services fournis aux «EuroGates», coûts associés à la garantie des services sur le réseau principal, coûts de la gestion de projet et coûts de la coordination générale) seront financés par IDA pour la durée des services.

- Un certain nombre d'accès de l'«EuroDomaine» aux réseaux administratifs nationaux dans les pays participants sont financés par IDA pour la durée du service.

  Un accès est compris comme incluant la boucle locale du réseau national à l'«EuroGate» ainsi que l'équipement de mise en réseau (routeur) et de sauvegarde associé. Il appartient à chaque État membre d'indiquer où ces connexions se feront.

  Le financement par IDA s'appliquera uniquement aux éléments fournis par l'opérateur de l'«EuroDomaine». Il ne couvre pas l'installation, le fonctionnement et la gestion de toute infrastructure gérée par ou pour le compte du domaine local.

- Les accès de l'«EuroDomaine» aux institutions européennes sont financés par IDA pour la durée du service.

- Les accès (installation et opération) des autres administrations sont financés par IDA pour une durée maximale d'un an. Au bout de l'année de service financé par IDA, l'administration pourra soit charger le fournisseur de service TESTA de poursuivre le service ou sélectionner tout autre fournisseur de services pour accéder à l'«EuroGate» le plus proche. (Le choix de l'administration dépendra entre autres choses des règles régissant les marchés publics.)

Informations complémentaires

6

6.1 Contacts

Pour contacter IDA au sujet d'un des aspects décrits ci-dessus, veuillez envoyer un message par courrier électronique à ida-central@cec.eu.int ou par télécopie au numéro: +32-2-2990286.

Pour contacter vos coordinateurs TESTA nationaux, envoyez vos messages électroniques à:

Allemagne

Coordinateur:
Sigurd Wilke
✉ SWilke@TIM.thueringen.de
☎ +49 361 379 3313
Contact technique:
Andreas Munde
✉ amunde@tlrz.thueringen.de
☎ +49 361 379 3313

Autriche

Coordinateur:
Leopold Koppensteiner
✉ Leopold.Koppensteiner@bmf.gv.at
☎ +43 1 71123-2525
Contact technique:
Michael Wickenhauser
✉ Michael.Wickenhauser@portal.at
☎ +43 664 1016853

Belgique

Coordinateur:
Plasschaert Roland
✉ roland.plasschaert@premier.fed.be
☎ +32 2 501 04 38

Danemark

Coordinateur:
Poul Bernt Jensen
✉ pbj@fsk.dk
☎ +45 3392 9886
Contact technique:
Henrik Lynnerup
✉ hlynncru@csc.dk
☎ +45 3614 6574

Espagne

Coordinateur:
Tomás Martín Rodrigo
✉ tomas.martin@sgci.dgopti.map.es
☎ +34 91 5861899
Contact technique:
Miguel A. Amutio Gómez
✉ miguel.amutio@sgci.dgopti.map.es
☎ +34 91 5862990

Finlande

Coordinateur:
Seppo Riihimaki
✉ Seppo.riihimaki@vnk.vn.fi
☎ +358 9 1602139
Contact technique:
Ville Hagelberg
✉ Ville.Hagelberg@vnk.vn.fi
☎ +358 9 1602137

France

Coordinateur:

Julien Français

✉ julien.francais@mtic.pm.gouv.fr

☎ +33 1 42755246

Grèce

Coordinateur & Contact technique:

Christos MOSCHONAS

✉ c.mos@syzefxis.gov.gr

☎ +30 1 9023713

Irlande

Coordinateur:

Tim Duggan

✉ tim_Duggan@cmod.finance.irlgov.ie

☎ +351 1 6045065

Contact technique:

Eddie McGinn

✉ eddie_mcginn@cmod.finance.gov.ie

Islande

Coordinateur:

Johann Gunnarsson

✉ johann.gunnarsson@fjr.stjr.is

Contact technique:

Bjorn Haraldsson

✉ bjorn.haraldsson@fjr.stjr.is

Italie

Coordinateur & Contact technique:

Marino Di Nillo

✉ mdinillo@centrotecnico.g-net.it

☎ +39 0685264453

Luxembourg

Coordinateur:

Daniel Nickels

✉ daniel.nickels@cie.etat.lu

☎ +352 49925 608

Contact technique:

Serge SPANIER

✉ serge.spanier@cie.etat.lu

☎ +352 49925 753

Norvège

Coordinateur:

Morten Rennesund

✉ morten.rennesund@ft.dep.telemax.no

☎ +47 22 24 99 13

Contact technique:

Erik Linnerud

✉ erik.linnerud@ft.dep.telemax.no

☎ +47 22 24 97 72

Pays Bas

Coordinateur:

Contact technique:

Portugal

Coordinateur & Contact technique:

Fernanda Costa

✉ fernanda.costa@inst-informatica.pt

☎ +351+21 4723189

Royaume-Uni

GSI Nerve Centre E-mail: gnc@ccta.gsi.gov.uk

Coordinateur:

Chris Simmons

✉ christopher.simmons@ccta.gsi.gov.uk

☎ +44 1424 432946

Contact technique:

Alan Collier

✉ alan.collier@ccta.gsi.gov.uk

☎ +44 1603 704400

Suède

Coordinateur & Contact technique:

Irene Andersson

✉ irene.andersson@statskontoret.se

☎ +46 8 454 4600

Pour les pays qui ne sont pas mentionnés, veuillez adresser vos demandes à ida-central@cec.eu.int.

6.2 Références

[Réf. 1] Décision n° 1719/1999/CE du Parlement européen et du Conseil, du 12 juillet 1999, définissant un ensemble d'orientations, ainsi que des projets d'intérêt commun, en matière de réseaux transeuropéens pour l'échange électronique de données entre administrations (IDA); Journal officiel L203 du 3.8.1999.

[Réf. 2] Décision n° 1720/1999/CE du Parlement européen et du Conseil, du 12 juillet 1999, adoptant un ensemble d'actions et de mesures visant à assurer l'interopérabilité de réseaux transeuropéens pour l'échange électronique de données entre administrations (IDA) et l'accès à ces réseaux; Journal officiel L 203 du 3.8.1999.

[Réf. 3] IDA Architecture Guidelines (Orientations pour l'architecture IDA)

[Réf. 4] How to Connect to TESTA

[Réf. 5] TESTA DNS HOW-TO

[Réf. 6] IP address allocation

[Réf. 7] TESTA mail services HOW-TO

[Réf. 8] Support assistance

[Réf. 9] How to make use of the TESTA portal

[Réf. 10] TESTA support procedures

[Réf. 11] How to use the TESTA hosting facilities

[Réf. 12] The IDA PKI infrastructure

A Member of the France Telecom Group

Global One Communications SA/NV
TESTA Contact
Avenue Louise 326 Bte 34
B-1050 Bruxelles, Belgique
tél.: +32 2 626 06 00
fax: +32 2 644 40 34
email: testa@globalone.net
http://www.globalone.net

Commission européenne, Direction Générale des Enterprises
Interchange of Data between Administrations (IDA programme)
Rue de la Loi 200
B-1049 Bruxelles, Belgique
email: ida-central@cec.eu.int
email: testa_infodesk@be.unisys.com
http://europa.eu.int/ISPO/ida/

Commission européenne
DIRECTION GÉNÉRALE DES ENTREPRISES