

# Espace Partenaires

## Guide Général de l'Espace Partenaires

Référence : DESU.GuideGeneral.E3.V1.3.doc

# Guide Général de l'Espace Partenaires

Destinataires	Projet / Organisme
Guillaume LE BESNERAIS	DGA/DQP/SDSI/PA
Franck DEVAUX	DGA/DQP/SDSI/PA
Patrice KRIER	DGA/DQP/CTSI
Bertrand FORLEN	DGA/DQP/SDSI/PA
Sabrina BISMUTH	DGA/DQP/SDSI/PA
Bertrand PINEL	IPPON Technologies
François PROT	IPPON Technologies
Alexandre KETTANEH	Phloème
Claude EIZENBERG	Phloème
Christian COATRINE	Phloème

### Visas avant diffusion externe

<b>Nom</b>	Alexandre KETTANEH	Bertrand PINEL
<b>Qualité</b>	Chef de Projet	Directeur de Projet
<b>Date</b>	30/01/06	30/01/06
<b>Visa</b>		

## SOMMAIRE

<b>1. INTRODUCTION .....</b>	<b>3</b>
<b>2. DÉFINITION ET FINALITÉS DE L'ESPACE PARTENAIRES .....</b>	<b>4</b>
<b>3. L'ORGANISATION DE L'ESPACE PARTENAIRES.....</b>	<b>6</b>
<b>4. LES UTILISATEURS DE L'ESPACE PARTENAIRES.....</b>	<b>7</b>
<b>5. LES SERVICES DE L'ESPACE PARTENAIRES .....</b>	<b>8</b>
5.1. PRÉSENTATION GÉNÉRALES DES SERVICES DE L'ESPACE PARTENAIRE .....	8
5.2. LES SERVICES DE L'ESPACE VISITEUR .....	8
5.3. LES SERVICES DE L'ESPACE MEMBRE.....	9
5.4. LES SERVICES OFFERTS DANS UNE COLLECTIVITÉ .....	9
<b>6. LA SÉCURITÉ INTERNE À L'ESPACE PARTENAIRES .....</b>	<b>10</b>
6.1. SÉCURISATION DU TRANSPORT .....	11
6.2. SÉCURISATION DU CONTENU DES MESSAGES .....	11
<b>7. LA DOCUMENTATION PROPRE À L'ESPACE PARTENAIRES .....</b>	<b>13</b>
<b>8. L'ACCÈS À L'ESPACE PARTENAIRES .....</b>	<b>14</b>
8.1. TYPOLOGIE DES RÉSEAUX DES PARTENAIRES .....	15

## 1. INTRODUCTION

---

Nous vous conseillons de consulter en premier lieu le document intitulé « Lexique » qui présente et décrit tous les termes utilisés dans ce présent document ce qui en facilitera la lecture.

Les mots explicités dans le « *Lexique* » sont *en italique*.

## 2. DÉFINITION ET FINALITÉS DE L'ESPACE PARTENAIRES

---

L'*Espace Partenaires (EP)* est une infrastructure qui offre des *services d'échange* sécurisés, de niveau sensible, entre *partenaires* étatiques et industriels du secteur de l'armement.

Grâce à l'*EP* des acteurs dispersés géographiquement partagent un environnement de travail commun où ils effectuent des transactions relatives à des contrats préétablis, communiquent, échangent entre eux des données et utilisent des applications.

L'*EP* a pour principal objectif de répondre aux besoins de dématérialisation et de travaux en mode collaboratif, entre les industriels de la défense et initialement la DGA.

Pour ce faire, l'*EP* dispose de services collaboratifs tels qu'une messagerie, des *forums*, des applications de type web, etc, ce dans le cadre sécurisé de communautés étanches et cloisonnées, et utilisables via un réseau informatique sûr, l'*ENX (European Network Exchange)*.

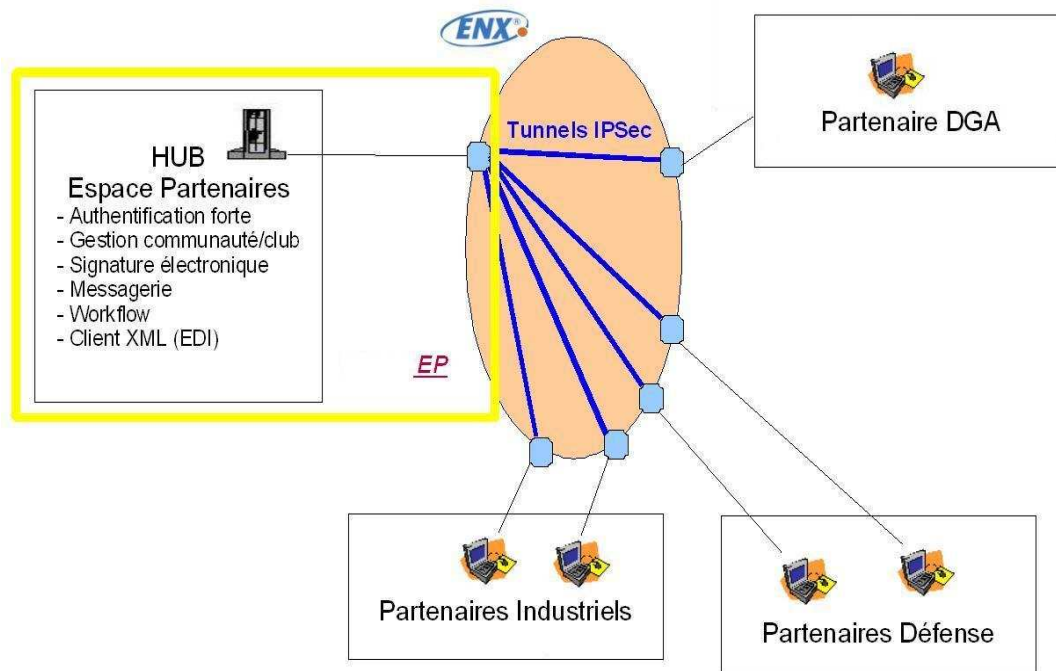
L'enjeu de l'*Espace Partenaires (EP)* se traduit par les finalités suivantes:

- contribuer à réduire les cycles de développement des programmes d'armement,
- développer et accélérer les flux d'information entre le ministère de la défense et ses partenaires en simplifiant les canaux de communication,
- simplifier et fluidifier les interconnexions entre les partenaires,
- permettre l'intégration de processus sur l'ensemble des filières conception, achats, logistique, après-vente, facturation/paiement entre le ministère de la défense et ses fournisseurs de tout rang.

Initialement envisagé pour améliorer les échanges d'information entre maîtrise d'ouvrage et industriels dans le cadre de programme d'armement, l'*EP* montre aujourd'hui un intérêt plus large qui dépasse le cadre des échanges au titre de programmes d'armement, pour devenir le lieu d'échange de toute nature entre les industriels d'une part et les entités étatiques de la Défense (forces armées, DGA, SIMMAD, SSF ...). Sur un plan technique l'*EP* fournit une solution d'échanges depuis les couches basses (remplacement des lignes dédiées vers les industriels) jusqu'aux plus hautes (couches applicatives à valeurs ajoutées).

Le dessin suivant exprime très synthétiquement le positionnement de l'*Espace Partenaires (EP)*.

(ce dessin sera revu pour une vue plus utilisateur)



### 3. L'ORGANISATION DE L'ESPACE PARTENAIRES

---

L'*Espace Partenaires (EP)* est structuré en plusieurs espaces cloisonnés différents par nature :

- Un *Espace Visiteur* qui est la seule zone publique accessible à tout un chacun sous réserve de disposer d'une connectivité à l'*EP*.
- Un *Espace Membre* qui est l'espace de travail réservé à chaque *membre EP* (cet espace présente aux *membres* le contenu de l'*EP* en respectant pour chacun d'entre eux ses droits et ses rôles).
- Des espaces thématiques les *collectivités* accessibles pour chaque *membre EP abonné*, via son *Espace Membre*

L'*Espace Visiteur* s'adresse en priorité aux acteurs des programmes d'Armement qui ne sont pas encore *membre* de l'*EP*. Sa nature première est pédagogique c'est à dire comprendre *pourquoi l'EP ?*, *pour qui ?*, *quel contenu ?*.

L'*Espace Membre*, point de départ de toute utilisation de l'*EP*, propose des *services* dont les objectifs principaux sont :

- Etablir un lien de communication entre tous les *membres de l'EP*.
- Animer l'*EP* par une communication permanente sur ses évolutions (nouveaux *services* ou concepts, technologies...) et son déploiement (nouveaux *partenaires*...).
- Simplifier et accélérer les échanges d'informations métier entre acteurs à l'aide des *services de l'EP* tels que la messagerie, les *workflows*, la recherche de contenu.
- Partager les savoirs aux moyens des *collectivités*, espaces thématiques auxquels le *membre est abonné*.

Chaque espace thématique appelé *collectivité* est une zone « cloisonnée » accessible aux seuls *membres EP abonnés* à cette *collectivité*, via leur *Espace Membre*. Il offre une collection de *services* qui répondent aux besoins d'une population d'acteurs d'un programme d'Armement qui ont un centre d'intérêt commun (par exemple: Maintenance du moteur M, Programme d'armement A,...).

## 4. LES UTILISATEURS DE L'ESPACE PARTENAIRES

---

Les utilisateurs cibles de l'*EP* sont en priorité les acteurs de la conception, de l'utilisation et du soutien des systèmes d'armes.

Sur un plan organique les utilisateurs dépendent tous d'un *partenaire* officiel de l'*EP*, industriel de la défense ou entité du ministère de la défense. La création d'un *partenaire* est de la responsabilité de l'administrateur central (*ACEP*) de l'*EP* (un collaborateur de la DGA).

Chaque *partenaire* doit désigner ses propres utilisateurs du système et assurer leur administration. Il est également responsable de l'administration des éventuelles applications qu'il a publiées sur l'*EP* et mises à disposition des autres *partenaires*.

La DGA est l'autorité qualifiée responsable de l'*EP*. A ce titre, elle a la charge de l'inscription de nouveaux *partenaires* et le cas échéant de leur enregistrement ENX.

L'accès et les usages de *EP* sont administrés et contrôlés par des *membres* auxquels sont attribués un ou plusieurs rôles tel que :

- *ACEP* Administrateur Central de l'*EP* qui assure une gestion adaptée à l'*EP* dans son ensemble (création d'une *collectivité*, d'un *partenaire*).
- *APEP* Administrateur d'un Partenaire de l'*EP* qui gère, pour son *partenaire*, les *services métiers*, les personnels, la création de nouveaux *groupes*, les informations privées...
- *AGEP* Administrateur d'un *groupe* de l'*EP* qui administre les propriétés (dont création et suppression) des *membres*, appartenant à ce *groupe*.
- *Modérateur* qui contrôle pour une *collectivité*, les *services*, les *abonnés* qui y accèdent, les *bulletins* et les *forums*...
- *Coordinateur* qui crée le modèle et son paramétrage pour un nouveau *scénario d'échange*.

## 5. LES SERVICES DE L'ESPACE PARTENAIRES

---

### 5.1. Présentation générales des services de l'Espace Partenaire

L'*EP* répond aux besoins de dématérialisation et de communication permanente, entre les industriels de la défense et initialement la DGA. Pour ce faire, l'*EP* propose des services d'échange collaboratifs :

- La consultation libre d'informations documentaires « publiques ».
- Une messagerie sécurisée et « cloisonnée » ce qui signifie que seuls les utilisateurs *membres de l'EP* ont une adresse mèl *EP*.
- Des *forums* « cloisonnés » au sein de *collectivités*, auxquels n'ont accès que les utilisateurs *abonnés*.
- Des ordonnancements automatiques et interactifs d'échanges entres différents utilisateurs ( *scénarios* ou « *workflow* »).
- Des applications de type web « publiées / référencées » dans l'*EP* et exploitées par les *partenaires*.
- La consultation, la modification et la publication, d'informations documentaires « cloisonnées » au sein d'une *collectivité*, réservées aux utilisateurs *abonnés* à cette *collectivité*.
- L'échange directe de fichiers vers un ou plusieurs utilisateurs désignés, avec purge sous 48 heures, pour des fichiers dont la taille est trop importante pour la messagerie.
- Service de signature et de notariation.

**Règle générale** : toute intervention d'un utilisateur sur l'*EP* est susceptible, par défaut, d'être soumise pour validation, a priori ou a posteriori, à un *modérateur* et / ou un *administrateur*.

### 5.2. Les Services de l'Espace Visiteur

L'*Espace Visiteur* propose aux utilisateurs *visiteurs* :

- La consultation d'informations non « sensibles » qui décrivent les apports de l'*EP* pour des *partenaires* potentiels et leurs acteurs...  
La finalité en est essentiellement pédagogique et vise à amplifier le champ d'application de l'*EP* vers de nouveaux besoins exprimés par les entités étatique et les industriels concernés par le progrès de l'Armement.
- L'accès au *formulaire* de demande d'adhésion à l'*EP* pour un nouveau *partenaire*.
- L'accès au *formulaire* de demande d'accès à l'*EP* par un *visiteur* qui souhaite devenir *membre*, et qui est collaborateur chez un *partenaire* déjà adhérent à l'*EP*.

### 5.3. Les Services de l'Espace Membre

Par des interactions très simples les *membres* de l'*EP* sont tenus informés des évolutions du portail *EP*.

Les services proposés sont les suivants:

- La consultation, la publication, d'informations générales réservées aux seuls *membres*.
- Le(s) *forum(s)* ouverts sur des sujets précis aux *membres EP*.

Chaque *membre* dispose d'un écran personnalisé (tableau de bord) qui l'informe sur :

- Les actions attendues concernant cet utilisateur.
- Les nouveaux mails reçus
- Les nouveaux messages dans des *forums* visibles par l'utilisateur.
- La liste des raccourcis définis pas le *membre*, pour tous les *services* qu'il souhaite retrouver rapidement.
- L'état d'avancement d'un *scénario* ou « *workflow* » dont il est acteur.
- La liste des *collectivités* auxquelles il est *abonné*.
- Les nouveaux *services*, les nouvelles *collectivités* qui lui sont accessibles

### 5.4. Les Services offerts dans une collectivité

Par des interactions très simples les *membres* abonnés à une *collectivité* accèdent au contenu thématique de cette *collectivité*, grâce aux *services* suivants:

- Accéder aux *bulletins* d'information de la *collectivité*, informations « sensibles » qui répondent aux besoins de l'animation et du travail collaboratif des *abonnés* de la *collectivité* (par exemple la présentation des activités de la *collectivité* depuis la dernière connexion de l'*abonné*).
- Création de liens d'accès immédiat à des informations (« bookmark »).
- Editer un *bulletin* d'information concernant la *collectivité*.
- Créer un message ou répondre dans un *forum* de la *collectivité*.
- Accéder à des *services métiers*, fournis par des applications gérées par des partenaires.

## 6. LA SÉCURITÉ INTERNE À L'ESPACE PARTENAIRES

La Politique de Sécurité Interne de l'Espace Partenaires (c.f. le document de référence PSI\_EP-V1.3 du 02/11/2005) a pour but la garantie des services rendus ainsi que la protection des biens et des informations sensibles. C'est la référence par rapport à laquelle toute évolution de l'*EP* devra être justifiée, que ce soit pour l'intégration d'un élément nouveau du système ou pour la modification d'un élément existant.

Elle fixe les obligations minimales applicables dans l'utilisation, l'exploitation, l'administration et l'évolution des services proposés par le système *EP* et répond aux principaux besoins suivants:

- La création d'un cadre général pour aider les personnes à élaborer et mettre en œuvre des mesures, des consignes et des procédures cohérentes en vue d'assurer la sécurité des systèmes d'information, et d'en simplifier l'usage pour tous les utilisateurs autorisés.
- Une authentification forte, établissant une relation biunivoque entre la personne physique qui utilise le système et l'utilisateur identifié est obligatoirement mise en place. Elle se base sur l'usage de certificats sur cartes à puces ou dispositifs USB. La présentation de ce certificat est strictement nécessaire pour s'identifier auprès du système.
- L'administration des droits d'accès par l'administrateur central EP pour ce qui concerne les partenaires, et par les partenaires eux même pour ce qui est de leurs utilisateurs.
- La gestion des moyens d'authentification fournis, soit par l'autorité qualifiée responsable de l'*EP*, soit par l'autorité qualifiée du *partenaire*, dès lors que l'autorité de certification du *partenaire* est compatible avec l'*EP*.  
Les autorités de certification actuellement opérationnelles sont Certinomis, Thales, Espace Partenaires. D'autres AC seront prochainement disponibles (DGA, Marine, Armée de l'air).
- La protection des contenus de l'*EP* (sauvegarde partielle quotidienne, archivage de l'ensemble du système tous les 6 mois).

Les informations échangées entre deux *partenaires EP* concernent des programmes d'armement, du MCO des systèmes d'arme, des sujets relatifs à la défense. L'*EP* contient en outre les informations, d'authentification des acteurs et des équipements, et d'administration et de gestion. Les informations échangées sont exclusivement des informations sensibles non classifiées de défense.

L'*EP* fournit aussi bien des services de sécurisation du transport des messages (liaisons ENX, HTTPS), que des services de sécurisation du contenu.

### 6.1. Sécurisation du transport

L'*Espace Partenaires (EP)* est au cœur d'un réseau en étoile reliant entre eux les différents *partenaires*.

L'*EP* se compose d'une plate-forme d'aiguillage et de mise en relation, le *HUB*, connecté au réseau sécurisé ENX. Il est accessible aux *partenaires* souhaitant l'exploiter, via ce seul réseau ENX.

La connexion entre un utilisateur et l'*EP* transite ainsi sur un réseau sécurisé. Cette connexion est renforcée par une liaison HTTPS qui garantit la confidentialité des échanges entre le poste de l'utilisateur et les serveurs de l'*EP*.

La publication d'un *service métier* en 'mode rebond' permet d'assurer la confidentialité des échanges entre le poste de l'utilisateur et l'application du *partenaire* qui supporte le *service métier*.

### 6.2. Sécurisation du contenu des messages

La signature d'un document garantit le contenu échangé, son intégrité, ainsi que sa provenance (non répudiation). Ce service global (en dehors de toute *collectivité*) est proposé aux utilisateurs *membres* de l'*EP*, et permet :

- d'assembler plusieurs fichiers dans une « enveloppe » et de la signer globalement. Cet assemblage est réalisé grâce à une archive ZIP ou à un autre format standard.
- à un utilisateur *membre* de l'*EP*, de vérifier la validité d'une signature apposée par un autre *membre*.

Dans le cadre des *scénarios d'échange*, le *coordinateur* peut exiger qu'un document soit signé à une étape du processus :

- Au moment de valider une telle étape, les données courantes du *formulaire* sont exportées vers le poste « client » de l'utilisateur afin de permettre le calcul de la signature et son renvoi à l'*EP*.
- Après validation de cette signature et du *certificat*, par l'*EP*, données et signature sont archivées et l'étape est validée.
- L'enregistrement de ces données sur les serveurs de l'*EP* permet le cas échéant de disposer d'une preuve irréfutable de l'action effectuée. L'utilisateur doit stocker sur son poste de travail un double de ces données et de la signature.

Le *notariat* est un service offert aux *membres* de l'*EP* leur permettant de conserver une empreinte et une signature de fichier sur les serveurs de l'*EP*. Elle permet de vérifier l'intégrité d'un document et de référencer et dater son enregistrement.

Cette fonction peut être liée de manière optionnelle à la fonction de signature de fichier.

Elle s'effectue en deux étapes :

- Une empreinte électronique est générée à partir du fichier cible sur le poste utilisateur. Elle est émise vers l'*EP* accompagnée d'une description libre du fichier (optionnelle).

Le pendant de cette fonction est l'interrogation de la base de notariat par un autre abonné afin de valider l'intégrité et l'origine d'un fichier.

- L'ensemble des données enregistrées par l'*EP* (empreinte, date et heure d'enregistrement, description libre) est transmise vers le poste utilisateur pour signature. Cette signature, une fois calculée est transmise à l'*EP* qui l'archive avec les données après avoir vérifié la validité du certificat utilisé.

## 7. LA DOCUMENTATION PROPRE À L'ESPACE PARTENAIRES

---

La documentation à disposition des utilisateurs comporte:

- Le présent Guide Général de l'Espace Partenaire qui présente les caractéristiques générales de l'*EP* et ses apports.
- Le Lexique Espace Partenaires qui définit les termes utilisés dans les Guides et Manuels.
- Le Guide personnalisé pour chaque *rôle* d'utilisateur.
- Le Manuel personnalisé pour chaque *scénario* complexe.

## 8. L'ACCÈS À L'ESPACE PARTENAIRES

---

Chaque utilisateur devra être identifié de manière unique pour accéder à l'*EP*. Aucun accès anonyme n'est autorisé. L'authentification des acteurs doit être conforme à la *PSI* de l'*EP*.

L'authentification sera réalisée à l'aide d'un support physique (carte à puce, clé USB, ...) protégé par un mot de passe propre à l'utilisateur.

La méthode de délivrance de ce medium personnel est la suivante:

*(processus à formaliser)*

Le réseau de transport imposé pour l'*EP* est ENX.

L'*EP* utilise les protocoles sécurisés d'échange web classiques HTTP(S), SMTP(S) et impose le chiffrement de bout en bout, au minimum SSL 128 bits, pour les échanges des données qu'il transporte (IPSec).

Il permet de mettre en relation des *partenaires* de toute l'Europe.

Un *partenaire* ne peut accéder à l'*EP* qu'en ayant une liaison physique le reliant au réseau utilisé par l'*EP*. Cette ouverture de liaison auprès d'un opérateur compatible avec la solution retenue ne peut se faire qu'après accord de la DGA, agissant en tant qu'autorité qualifiée responsable de l'*EP*.

Les *partenaires* ont à charge leur connexion au réseau ENX ainsi que l'accès au *Hub* de l'*EP*. Il est du ressort des *partenaires* de définir et de réaliser l'interface entre son intranet et le point d'accès à l'*EP* en conformité avec les dispositions de la *PSI* et du protocole d'accord qu'ils ont approuvés.

### 8.1. Typologie des réseaux des partenaires

Il existe trois architectures réseaux possible, permettant à un *partenaire* de configurer des postes de travail connectés à l'*EP*.

<b>Architecture</b>	<b>Poste relié à</b>	<b>Remarques</b>
Postes isolés	Routeur ENX	Les postes sont reliés via un <i>hub</i> au routeur ENX, et disposent d'adresses publiques. Tous les postes de travail sont visibles à partir de l' <i>EP</i> . Les serveurs hébergeant les <i>services métiers</i> peuvent être ainsi directement reliés. Le <i>partenaire</i> respectera la <i>PSI</i> de l' <i>EP</i> .
Réseau local isolé	Routeur / Switch, lui même relié au routeur ENX.	Le réseau des postes de travail n'est pas sur le même plan d'adressage que celui d'ENX. Le réseau n'est pas connecté à celui de l'entreprise. Les postes seront tous vus par l' <i>EP</i> avec la même adresse IP. Pour rendre accessible un <i>service métier</i> , il faut le connecter en poste isolé (première architecture) ou configurer le routeur/switch pour le rendre accessible s'il est situé dans le réseau local. Une protection du réseau local est recommandée. Le <i>partenaire</i> respectera la <i>PSI</i> de l' <i>EP</i> .
Interconnexion au réseau d'entreprise.	Routeur / Switch, lui même relié au routeur ENX.	Le <i>partenaire</i> pourra mettre en place une passerelle permettant d'interconnecter son réseau à celui de l' <i>EP</i> . Il est nécessaire de prévoir un sécurisation de l'architecture réseau avec au moins un firewall. Le comportement sera identique à celui de l'architecture en réseau local isolé. Il en est de même pour les <i>services métier</i> . Le <i>partenaire</i> respectera la <i>PSI</i> de l' <i>EP</i> .