Centre national de la recherche scientifique
Direction des systèmes d'information

Sécurité et EAI

Référence : NOT03K009DSI

Date : 09/07/2003

Version : 1.0

Auteurs : David ROUSSE (DSI/BEST) et Véronique LONGUEVILLE (DSI/BBFC)

Diffusion : DSI

Objet du document : Apports d'une infrastructure EAI en termes de sécurité du SI

Table des mises à jour du document

Version	Date	Objet de la mise à jour
1.0	09/07/2003	Création du document

Sommaire

1 INTRODUCTION

L'EAI permet de synchroniser et de faire communiquer des applications hétérogènes par échange d'informations indépendamment des plates-formes et du format des données. L'EAI fournit un support pour le suivi et la maîtrise de l'évolution du système d'information et intègre certaines fonctions inhérentes à la sécurité, renforçant par là même sa position au sein du SI.

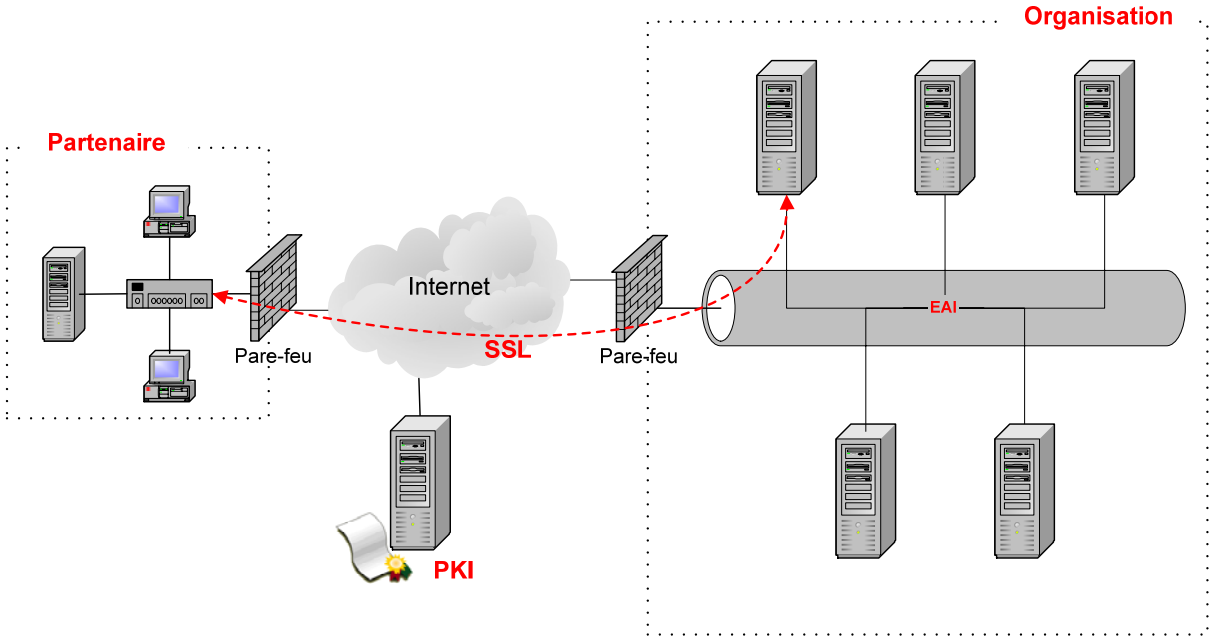

Figure 1 : aperçu d'une solution d'EAI dans un SI

En partant du schéma généraliste présenté ci-dessus, les paragraphes qui suivent ont pour objectif :

- de mettre en évidence les fonctions de sécurité qu'une solution d'EAI peut apporter à un SI en termes de :
  - sécurisation des flux.
  - sécurisation des fonctions d'administration et d'exploitation.
  - sécurisation de l'utilisation des Web Services.

- de présenter des exemples concrets de mise en œuvre possible des fonctions sécurité d'un EAI :
  - au sein du SI du CNRS (au regard des besoins déjà identifiés).
  - dans d'autres organisations (retour d'expérience des applications en production chez Groupama).

2 SECURITE DES FLUX

2.1 Problématique générale

La plupart des flux de données échangés entre applications du SI CNRS reposent aujourd'hui sur des transferts de fichiers. La sécurité est souvent implantée par la notion de login/password, parfois inscrits en clair dans des fichiers batch.

Une infrastructure d'EAI offre les services de sécurité suivants :

- l'authentification (d'un flux ou de chaque message), l'intégrité, la confidentialité et la garantie de non répudiation des données échangées au sein du SI ou avec l'extérieur.

- la gestion des habilitations qui permet de répondre à des questions du type : le message émis par l'application X est-il autorisé ? Si oui, est-il valide en terme de format et de valeurs des données ?

- un référentiel des émetteurs et destinataires (machines, personnes) est fourni par certaines solutions EAI via des Access Control List sur les différentes typologies de flux.

- un flux peut être signé ou crypté soit dans sa globalité, soit par message.

2.2 L'EAI, VPN au niveau métier

2.2.1 Vue d'ensemble

L'essence même de l'EAI est de décorréler les applications entre elles. Chaque application communique directement avec l'EAI, qui se charge d'acheminer les informations qu'il reçoit vers les applications destinatrices. L'EAI peut être vu comme un bus à travers lequel différentes entités vont communiquer. Ce bus va assurer diverses fonctions (transport, transformation, routage et workflow) ainsi que les services de sécurité.

L'EAI crée un tunnel sécurisé, il décharge les entités en présence (applications, utilisateurs) de plusieurs tâches relatives aux services de sécurité. Il peut être vu comme un VPN intelligent grâce aux fonctions de sécurité qu'il prend en charge (qui sont de plus haut niveau que ceux des VPN classiques du monde réseau).

Cependant cela n'est pas sans implications sur la PKI et les certificats des entités en présence, et ce sur 2 points:

- dans un cadre EAI intra-organisation, les applications ou les personnes doivent disposer de certificats relatifs aux fonctions qu'elles assument. Lors de la mise en place d'un workflow, il faut également s'assurer que les certificats sont supportés par tous les acteurs de ce workflow (si un seul maillon de la chaîne du workflow n'est pas certifié, la sécurité n'est plus assurée).

- dans un contexte inter-organisations, les échanges entre les organisations concernées doivent se faire en toute confiance. Pour cela, il faut utiliser des certificats délivrés par une autorité tierce au nom des entreprises (ou bien par un échange de certificats racine entre les PKI des différentes organisations). Chaque intervenant se doit de supporter l'utilisation des certificats, et ces certificats doivent être compatibles en termes de confiance, de format des champs spécifiques et de politique de certification. Une solution envisageable est le recours à une autorité de certification reconnue de tous pour éviter tout problème (incompatibilités techniques de champs spécifiques X.509, différence dans les algorithmes de chiffrement utilisés, multiplication des CRL, …).

La question suivante se pose alors : l'EAI peut-il comprendre les messages ou ne fait-il que du routage de messages chiffrés et signés ?

2.2.2 L'EAI, simple outil de routage

Dans le cas où l'EAI ne peut comprendre les messages, il agit comme La Poste : le seul véritable service rendu est la garantie de livraison des messages.

Ce scénario peut rapidement devenir ingérable : pour envoyer un message chiffré que l'EAI ne pourra déchiffrer, il faut aller récupérer la clé publique du destinataire. Cela oblige l'émetteur à effectuer une partie du routage et à structurer de manière complexe ses messages en effectuant notamment une tâche de pré-formatage en fonction des destinataires, tâche normalement dévolue à l'EAI.

2.2.3 L'EAI, VPN intelligent

Au regard des problèmes potentiels évoqués au paragraphe précédent, il est préférable de rester dans le cadre de l'architecture EAI en utilisant la clé publique de l'EAI pour le chiffrement, et seulement celle-ci. Ainsi l'EAI effectue l'intégralité des tâches et décharge réellement ses interlocuteurs du routage, des formats, et de la connexion.

L'EAI apparaît donc comme un VPN intelligent en mutualisant des services de sécurité de haut niveau (notaire, horodatage, vérification de la validité de certificats, garantie de livraison, confidentialité, intégrité).

Cependant, il faut noter que les fonctions présentées ci-dessus sont souvent réalisées au plus bas niveau de l'architecture EAI, c'est-à-dire dans la couche transport MOM (qu'intègrent les outils EAI). Par exemple, Candle MQSecure gère l'authentification, l'intégrité et la confidentialité des messages d'IBM MQSeries. Microsoft MSMQ offre quant à lui la possibilité de contrôler les accès sur les files d'attente et de gérer la confidentialité et l'intégrité des messages, alors que les fonctions d'authentification viennent du système d'exploitation Microsoft Windows.

2.3 L'EAI, firewall au niveau métier

Dans un cadre inter-organisations principalement, l'EAI peut apparaître comme un élément de sécurité à part entière et devenir partie intégrante de la politique et de l'architecture de sécurité puisqu' il peut assurer des fonctions de contrôle d'accès et d'habilitations de haut niveau.

Les outils de contrôle d'accès assurent généralement du filtrage bas niveau (filtrage de paquets, de ports et de protocoles par exemple). Certains outils remontent au niveau applicatif, avec des filtres anti-virus sur les mails, la recherche des virus dans les fichiers compressés et l'analyse de contenu des messages. Cela demeure cependant du filtrage technique et non applicatif. L'utilisation de l'EAI comme outil de filtrage peut permettre de donner une orientation métier à la fonction de contrôle d'accès.

En frontal avec l'extérieur, l'EAI est capable de refuser l'entrée dans le système d'information à certains flux en fonction de leur signature (certificats non valides, provenance non reconnue, Autorité de Certification douteuse, …), mais aussi en fonction de la non validité des messages (format incorrect ou obsolète). Ainsi, l'EAI apparaît comme un outil de filtrage situé non plus au niveau technique du contrôle d'accès mais au niveau métier.

D'un point de vue technique, il est possible d'imaginer une architecture fondée sur deux instances d'EAI, l'une localisée en DMZ et en contact avec l'extérieur, et l'autre placée dans l'Intranet (MZ). L'instance sécurisée en Intranet ne voit hors de sa zone que l'instance en DMZ. L'instance en DMZ ne communique qu'avec l'instance en MZ et effectue tous les filtrages évoqués précédemment comme un véritable « firewall métier » (avec des filtrages sur l'identité des interlocuteurs, sur le format des messages, sur le contenu des messages). En schématisant, on peut imaginer le scénario suivant :

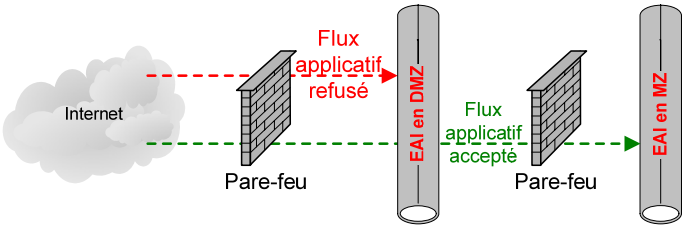

Figure 2 : l'EAI, firewall sur les flux de données

Remarque : la criticité des informations permettant des contrôles et situées en DMZ doit évidemment être évaluée avant toute mise en place de filtrages. Il n'est par exemple pas envisageable de stocker en DMZ une information à caractère confidentiel.

3 SECURITE DE L'ADMINISTRATION ET DE L'EXPLOITATION

L'un des apports d'une solution d'EAI est la facilité d'administration et d'exploitation (suivi détaillé des flux inter-applicatifs, intégrité transactionnelle maîtrisée).
Le bus de communication unique fourni par l'EAI donne une vision globale des données échangées entre applications.

Les points à retenir sont les suivants :

- le paramétrage et la configuration des flux de données peuvent se faire pour certains outils de manière graphique.

– la supervision (suivi des flux, gestion de la QoS, gestion des alarmes orientées métier) est possible tant au niveau des infrastructures techniques d'échanges de l'EAI (l'équivalent des outils de supervision réseau mais placé au niveau applicatif) qu'au niveau métier (à destination de l'utilisateur final).

En conclusion, une infrastructure d'EAI permet à un Information Flow Administrator de faire l'équivalent des activités d'un Database Administrator au niveau des flux de données et sécurise les flux de données du SI. Ainsi, il est possible de gérer le dialogue applicatif, en sachant « qui dit quoi comment à qui et quand ».

4 SECURITE, EAI ET WEB SERVICES

Il est indéniable que les Web Services ont un fort potentiel pour accroître l'interopérabilité des applications.

Cependant, choisir les Web Services comme outil unique de communication pour une application pénalise fortement l'évolutivité et la souplesse de celle-ci (pour utiliser ou exposer un Web Services, il faut du code ….), d'autant que la version actuelle de la norme des Web Services n'est pas encore stabilisée et va évoluer, notamment pour intégrer la notion de sécurité (le danger serait de devoir maintenir rapidement le code applicatif dédié à la communication).

Une solution alternative est d'utiliser les Web Services dans le cadre d'une infrastructure EAI. En effet, les EAI permettent de mettre en place des Web Services rapidement (exposition d'un service Web ou accès à un service Web). Cela permet de centraliser les problématiques d'interfaçage dans un outil d'EAI et de ne conserver dans les applications que les aspects purement métier. L'EAI s'allie donc harmonieusement avec les Web Services, ces derniers offrant aux outils d'EAI un connecteur potentiellement universel, mis en œuvre simplement via l'infrastructure EAI.

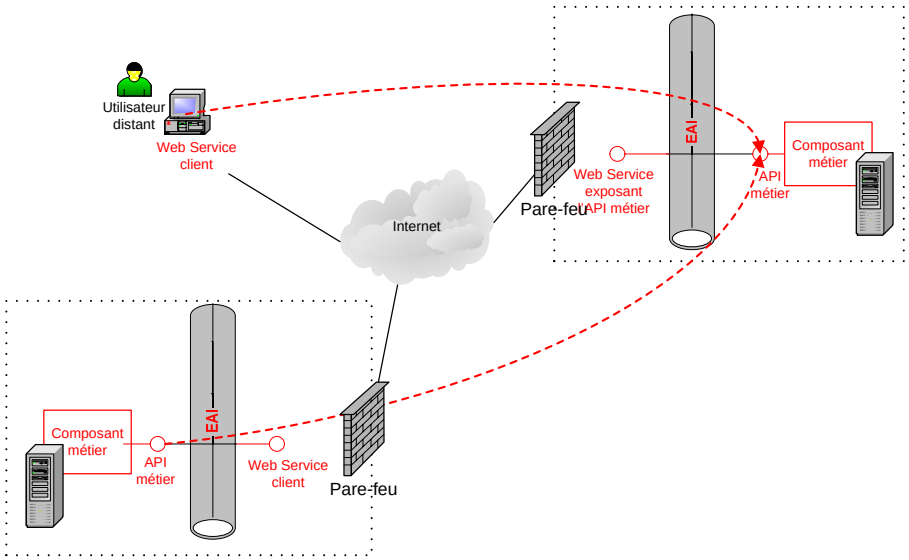

Figure 3 : utilisation des Web Services via une infrastructure EAI

Un exemple de solution pragmatique applicable actuellement est d'utiliser la sécurité via des protocoles réseaux de type IPSec sur lesquels faire passer des Web Services communiquant entre EAI, les applications sources et cibles contentant seulement du code métier (le code dédié au middleware choisi, par exemple les Web Services, est déporté dans l'EAI).

5 EXEMPLES DE MISE EN ŒUVRE DES FONCTIONS SECURITE D'UN EAI

5.1 Besoins existants au CNRS

Des besoins réels existent actuellement au sein du SI du CNRS. On peut noter les échanges ETEBAC3 entre le CNRS et le Trésor Public de Chalons d'une part, entre le CNRS et la Banque de France d'autre part, qui se font aujourd'hui avec deux logiciels différents (respectivement SAGE Banque Paiement 500 et PostBanque), depuis un réseau bureautique dont la sécurité d'accès est minimale. Les solutions mises en œuvre actuellement sont à l'évidence peu sûres en terme technologique (ETEBAC3 n'assure ni intégrité, ni confidentialité) et en terme organisationnel. Entre autres faiblesses, les logiciels de transfert sont installés sur des postes utilisateurs dont la sécurité d'accès dépend de la politique générale de sécurité de la DR (on pourra se reporter au document spécifique sur le sujet pour une vision plus large des faibles mesures de sécurité offertes par la solution actuelle de télétransmissions ETEBAC3).

Le schéma page suivante illustre comment une solution d'EAI pourrait sécuriser et rationaliser les télétransmissions ETEBAC3.

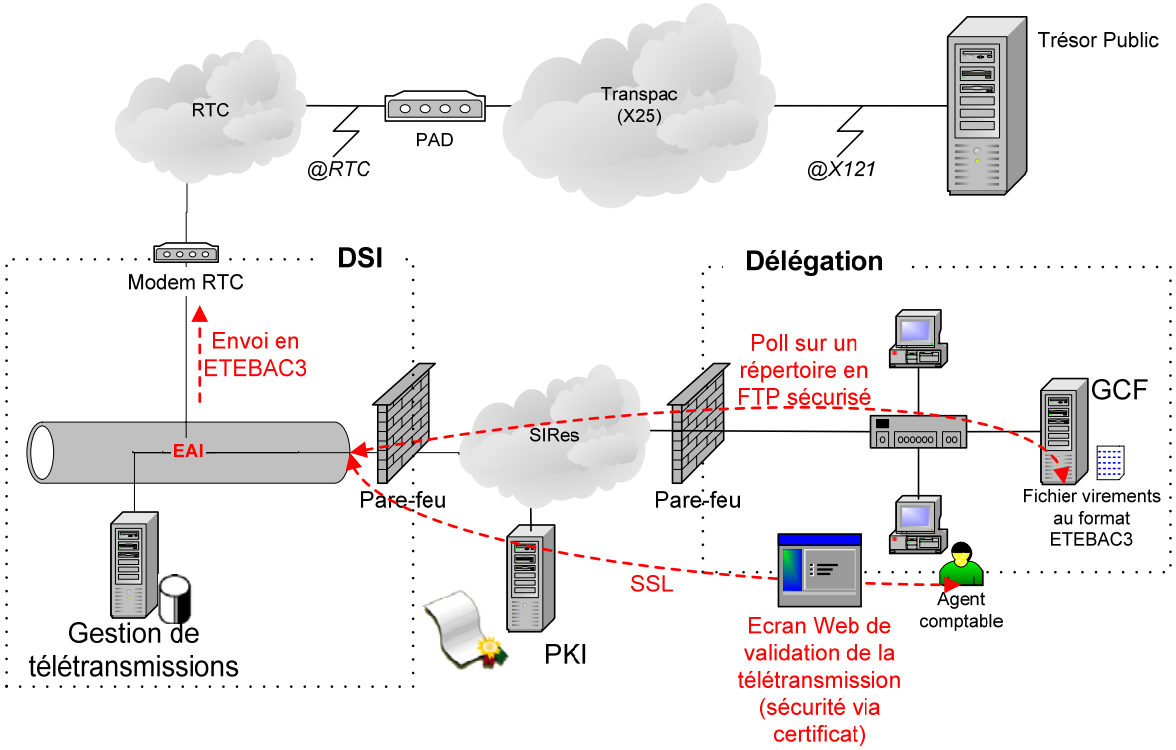

Figure 4 : télétransmissions ETEBAC3 ET EAI

Par ailleurs, des besoins de télétransmissions sont identifiés pour la fin de l'année 2003 :

- via le protocole CFT vers la DIT de Bordeaux.
- pour remplacer le transfert manuel de bandes magnétiques d'ICARE/POPART vers la BNP en ETEBAC3.
- pour permettre au BPAT et aux Marins de l'INSU de remplacer les envois de disquettes vers la Poste par une télétransmission en ETEBAC3.

Il est possible d'ajouter aux flux ETEBAC3 présentés sur la figure 4 les envois de données mentionnés ci-dessus : l'EAI serait ainsi la plaque tournante des télétransmissions réalisées par le CNRS, et la gestion de ces différents flux serait améliorée et sécurisée (cette solution éliminerait notamment les problèmes de gestion de la sécurité spécifiques à chaque DR).

5.2 Un exemple opérationnel, le retour d'expérience de GROUPAMA

GROUPAMA a mis en place une architecture d'EAI (basée sur l'outil BusinessWare de VITRIA), qui a permis notamment d'automatiser et de sécuriser les échanges de données dans le cadre de la prise en charge d'un assuré ayant subi un sinistre. Cette mise en place est marquée par la décentralisation des acteurs inclus dans le processus. Avant la mise en place de l'EAI, le processus était le suivant :

- appel téléphonique de l'assuré au centre régional Groupama qui enregistre le sinistre dans son système d'information local.
- transfert par fax d'une mission à un prestataire qui affecte un dépanneur à la mission, rappelle l'assuré, enregistre la mission dans son système d'information et retransmet les informations au centre régional (avec un temps de traitement d'une mission imposé au prestataire d'au maximum 15 minutes).

Le but du projet a été d'automatiser les échanges entre les centres régionaux et les prestataires :

- envoi automatique d'une mission dans la boîte aux lettres du prestataire dès que la mission est créée par le centre régional dans son SI.
- traitement de la mission par le prestataire (sélection d'un dépanneur) via une IHM adaptée, avec une validation de l'utilisateur par certificat numérique, puis retour automatique des informations au centre régional après traitement par le prestataire.

La solution technique retenue pour le projet devait respecter les contraintes suivantes, en plus de la sécurisation des flux échangés :

- communication asynchrone de faibles volumes de données.
- rapidité des flux.
- aucune installation d'application cliente ni de plate-forme imposée chez le prestataire (utilisation de formulaires Web pour la saisie des données de la mission en Extranet par le prestataire).
- non-intrusivité de l'EAI dans les applications back-office des centres régionaux.

6 CONCLUSION

L'EAI peut être vu comme un outil de sécurité au niveau métier. Il fait remonter dans les couches applicatives les fonctions classiques de sécurité situées habituellement dans les couches techniques et réseau.
De plus, l'EAI centralise et facilite la mise en place de la sécurité. En mutualisant différents services de sécurité, l'architecture EAI offre de manière transparente ces services en les intégrant dans un workflow.
En conclusion, l'EAI, en tant que bus d'échange du SI, peut devenir une autorité de référence en matière de sécurité à laquelle les applications et les utilisateurs peuvent faire confiance.

7 GLOSSAIRE

ACL Access Control List
CFT Cross File Transfer
CRL Certificate Revocation List
DMZ Demilitarized Zone
EAI Enterprise Application Integration
MOM Middleware Oriented Message
MZ Militarized Zone
PKI Public Key Infrastructure
QoS Quality of Service
SSL Secure Socket Layer
VPN Virtual Private Network