



## Sécurisation des conférences avec DataConf

### Préambule

Le système actuel utilise le protocole RFB/TCP pour l'échange des données d'information qui permettent de retransmettre l'écran du conférencier.

Ce sont ces données qui font l'objet des échanges "métiers" entre les utilisateurs du système : lorsque deux personnes échangent des informations autour d'un document technique (le schéma électrique d'un prototype, le plan d'un aménagement urbain etc...) les informations correspondantes, souvent confidentielles, transitent sur l'interconnexion.

*Dans une conférence non cryptée*, le format d'échange de ces données les rend difficilement exploitable par un utilisateur malveillant : le document technique n'est en effet pas échangé en tant que tel. Ce qui circule est constitué de (petits) blocs d'informations graphiques comprimées. Chacun représente une portion d'écran repérée par l'application du conférencier comme devant faire l'objet d'un rafraîchissement. Plusieurs heuristiques et algorithmes d'encodage, d'optimisation ou de compression viennent compliquer cette approche : ces différentes options sont négociées entre l'application du conférencier et chaque application de participant lors de l'initialisation.

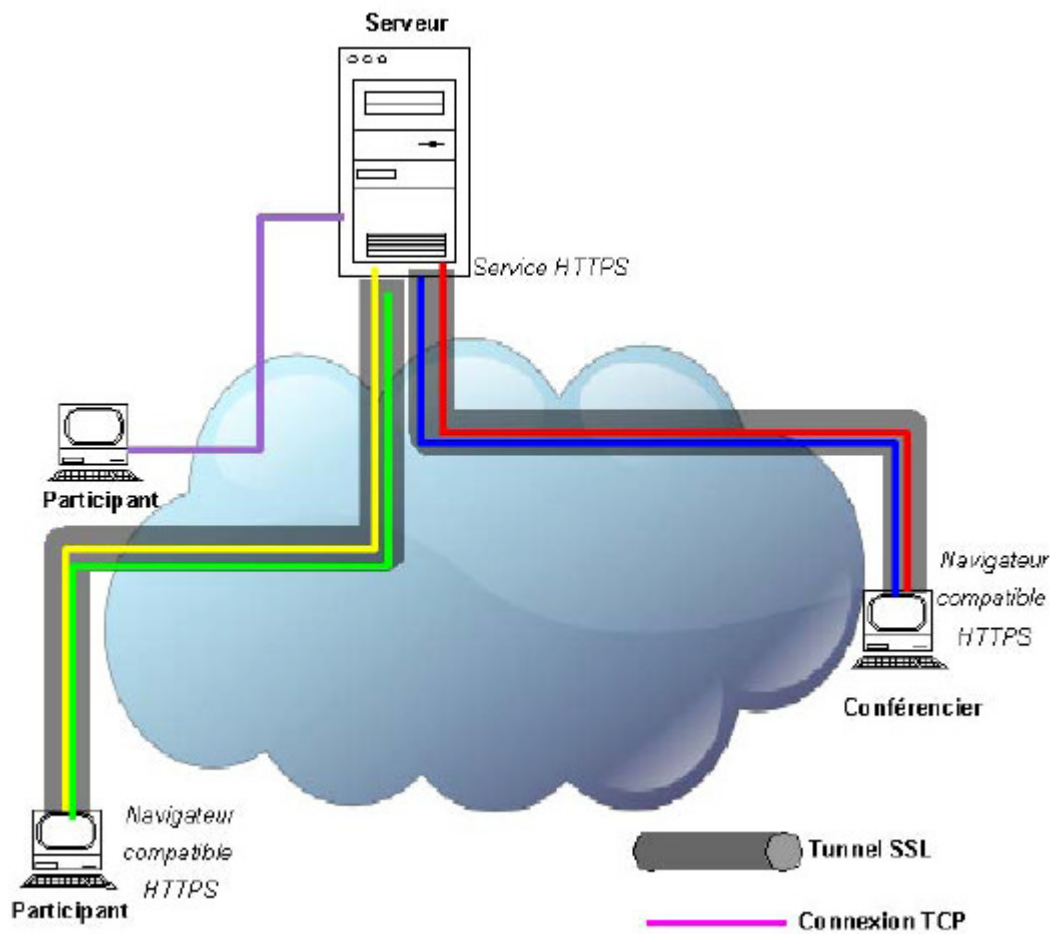
Dans l'hypothèse où un utilisateur malveillant arriverait néanmoins à reconstituer le document technique faisant l'objet de la session de travail collaboratif, il ne disposerait pas du document lui-même mais, dans le meilleur ou, selon le point de vue adopté, le pire des cas, d'une représentation graphique de ce dernier (c'est la différence entre posséder, sous la forme d'un fichier AutoCad par exemple, le document technique et en posséder une de ses représentations sous forme d'image souvent partielle).

Cet état de fait constitue déjà un certain niveau de protection des données mais pour certaines utilisations sensibles ce niveau de protection se révèle encore insuffisant. C'est pourquoi nous avons développé un système qui permet de crypter les conférences DataConf.

*Dans une conférence cryptée*, DataConf utilise le protocole SSLv3 pour encoder les données (cf. figure 1). Ce protocole est le même que celui utilisé pour les transactions bancaires sur internet. Le codage sur 128 bits vous garantit que vos données ne pourront pas être décodées.

# RasterTech

*"giving you the right image"*



**Fig 1 : Schéma d'une conférence sécurisée**

## Crypter sa conférence DataConf

Pour crypter une conférence, le conférencier doit choisir cette option avant le lancement de celle-ci. Pour cela il clique simplement sur la case à cocher « Voulez-vous un connexion sécurisée (SSL) ? » (cf. figure 2).

Pour que la conférence soit entièrement sécurisée, les participants doivent aussi cocher cette option lors de leur connexion à la conférence.

Paramètres de connexion	
Voulez-vous une connexion sécurisée (SSL) ? <input type="checkbox"/>	Etes-vous derrière un pare-feu (Firewall) ? <input type="checkbox"/>
Utilisez-vous un proxy ? <input type="checkbox"/>	Hôte Proxy : <input type="text"/>
	Port Proxy : <input type="text"/>
	Proxy Username : <input type="text"/>
	Proxy Password : <input type="text"/>

Paramètres de la conférence	
Port de la conférence : <input type="text"/>	Pseudo : <input type="text"/>
Code de la conférence : <input type="text"/>	Email : <input type="text"/>

**Fig 2 : Copie de l'interface DataConf**