CredSSP

Aurélien Bordes
aurelien26@free.fr

OSSIR – 13 juillet 2010
v2.0

RDP (Remote Desktop Protocol)

- Solution d'accès distant via un déport :
  - de l'affichage graphique du serveur vers le client
  - des entrées du client vers le serveur
- Historique des versions :
  - 4.0 : Windows NT 4 Terminal Services
  - 5.0 : Windows 2000
  - 5.1 : Windows XP
  - 6.0 : Windows Vista
  - 6.1 : Windows 2008
  - 7.0 : Windows 7 / 2008R2

Extensions

- RDP permet également d'utiliser de nombreuses extensions :

- Multiparty Virtual Channel
- Clipboard Virtual Channel
- Audio Output Virtual Channel
- Remote Programs Virtual Channel
- Dynamic Channel Virtual Channel
- File System Virtual Channel
- Serial Port Virtual Channel
- Print Virtual Channel
- Smart Card Virtual Channel
- XPS Printing Virtual Channel
- Plug and Play Devices Virtual Channel
- Video Virtual Channel
- Audio Input Virtual Channel
- Composited Remoting V2
- Licensing
- Session Selection
- Graphics Device Interface (GDI) Acceleration
- Desktop Composition
- Remote Programs Virtual Channel
- NSCode
- RemoteFX Codec

Sécurité de RDP

- Standard RDP Security :
  - **`encryptionMethods`** :
    - Null, 40 bits, 56 bits, 128 bits ou FIPS
  - **`encryptionLevel`** :

Level	C ⇨ S	S ⇨ C	Choix méthode	Algo. chiffrement	Key Exch. MAC
Low	Chiffré	Clair	Max. client	RC4	MD5/SHA1
Client Compatible	Chiffré	**Chiffré**	Max. client	RC4	MD5/SHA1
High	Chiffré	Chiffré	**Max. serveur**	RC4	MD5/SHA1
Fips	Chiffré	Chiffré	N/A	**3DES**	**SHA1**

Sécurité de RDP

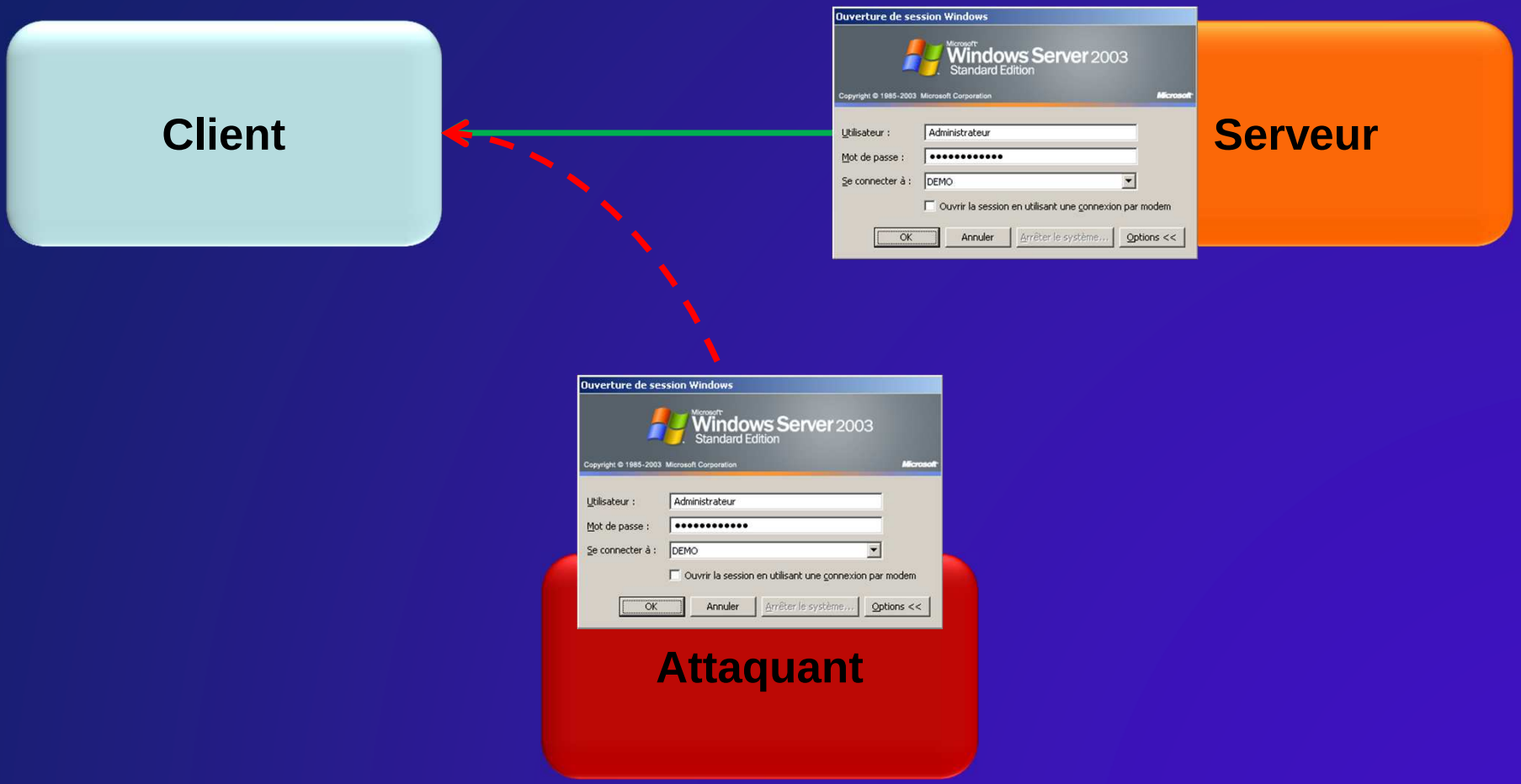
- Échanges des clefs :

Authentification dans RDP

- Le client s'authentifie après du serveur via ses *credentials* qu'il fournit (authentification classique Windows)

- L'authentification du serveur vis-à-vis du client n'a pas été initialement prise en compte :
  - Bugtraq (02/04/2003) : *Microsoft Terminal Services vulnerable to MITM-attacks*

Scénario de détournement



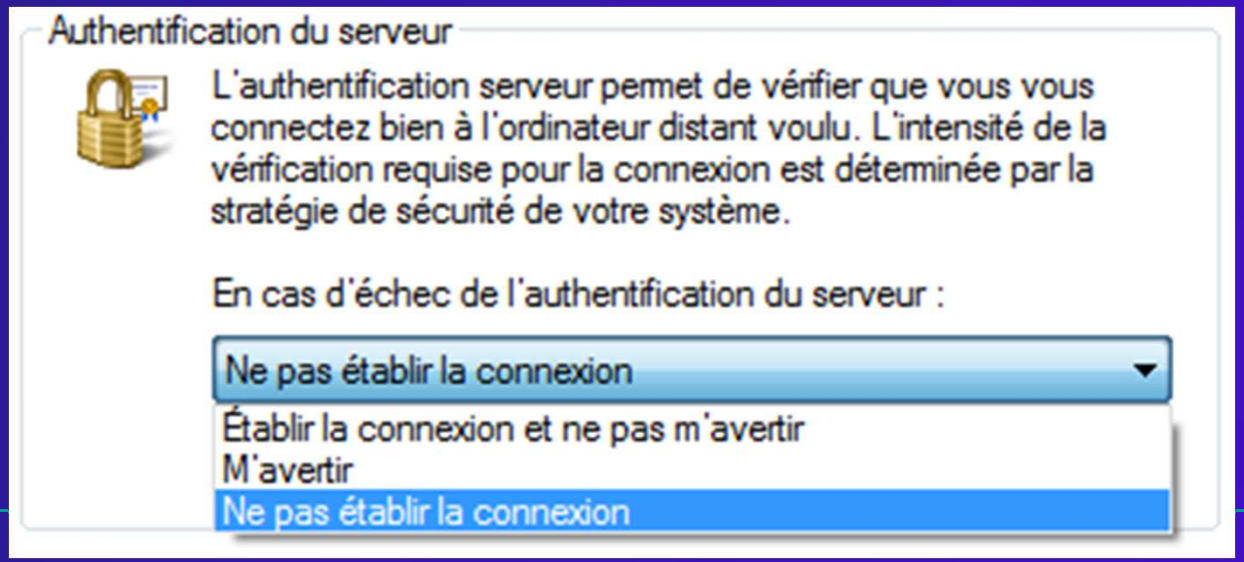
Premier essai…

- Utilisation d'un certificat pour transporter **K** (messages de type **`CERT_CHAIN_VERSION_2`**)
  - Certificat dans :

    `HKLM\SYSTEM\CurrentControlSet\Services\TermService\Parameters\Certificate`
  - Clef privée associée dans **`L$HYDRAENCKEY`**
- Ce certificat est signé par une clef privée codée en dur (**`mstlsapi.dll`**) :
  - SecuriTeam (02/06/2005) : *Microsoft RDP Man in the Middle Vulnerability*

Deuxième essai

- Il est possible d'utiliser un certificat issu d'une chaîne de certification en lieu et place du certificat auto-généré
- **Recommandation** :
  - Mettre à jour son client vers la dernière version
  - Imposer au client la validation du certificat présenté par le serveur



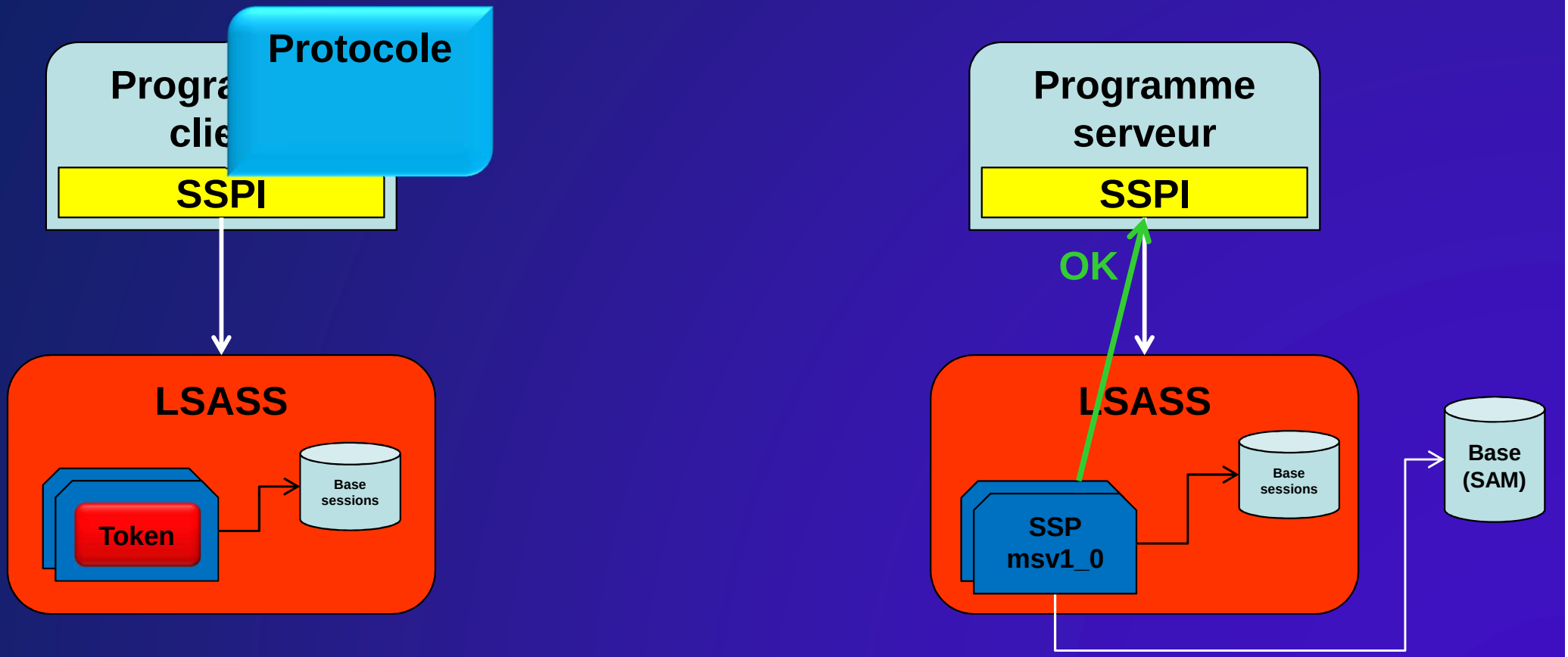
Enhanced RDP Security

- Changement complet des méthodes :
  - d'authentification client/serveur
  - de chiffrement et d'intégrité des messages RDP
- Toutes les fonctions de sécurité sont déléguées à un SSP (*Security Support Provider*)
- Pour RDP, il est possible d'utiliser :
  - **`PROTOCOL_SSL`** : Schannel
  - **`PROTOCOL_HYBRID`** : CredSSP

Rôles d'un SSP (*Security Support Provider*)

- Authentification Client / Serveur
- Chiffrement de messages (PRIVACY) :
  - EncryptMessage
  - DecryptMessage
- Signature de messages (INTEGRITY) :
  - MakeSignature
  - VerifySignature

Échanges SSP



Principaux SSP

- NTLM
  - protocoles LM et NTLM
- Kerberos
- **Negotiate (SPNego)**
  - **GSS-API et SPNego**
  - **Négociation de NTLM ou Kerberos**
- **Schannel**
  - **SSL/TLS**
- **CredSSP**
  - **Utilisation de Schannel et SPNego**

Modes d’utilisation

- Utilisation d’une *Security-Enhanced Connection Sequence*

- Deux modes d’utilisation :
  - ***Negotiation-based*** : négociation de l’extension de sécurité dans les messages RDP
  - ***Direct*** : utilisation de l’extension de sécurité avant les messages RDP

Modes d’utilisation

Negotiation-based security-enhanced connection sequence

Direct security-enhanced connection sequence

CredSSP

- CredSSP est un SSP (*Security Service Provider*) apparu avec Vista et 2008 (activé par défaut)
- CredSSP est également disponible sur XP depuis le SP3 (mais n'est pas activé par défaut)
- CredSSP est principalement utilisé par le service de connexion au bureau à distance (Terminal Services) afin de renforcer l'authentification client/serveur

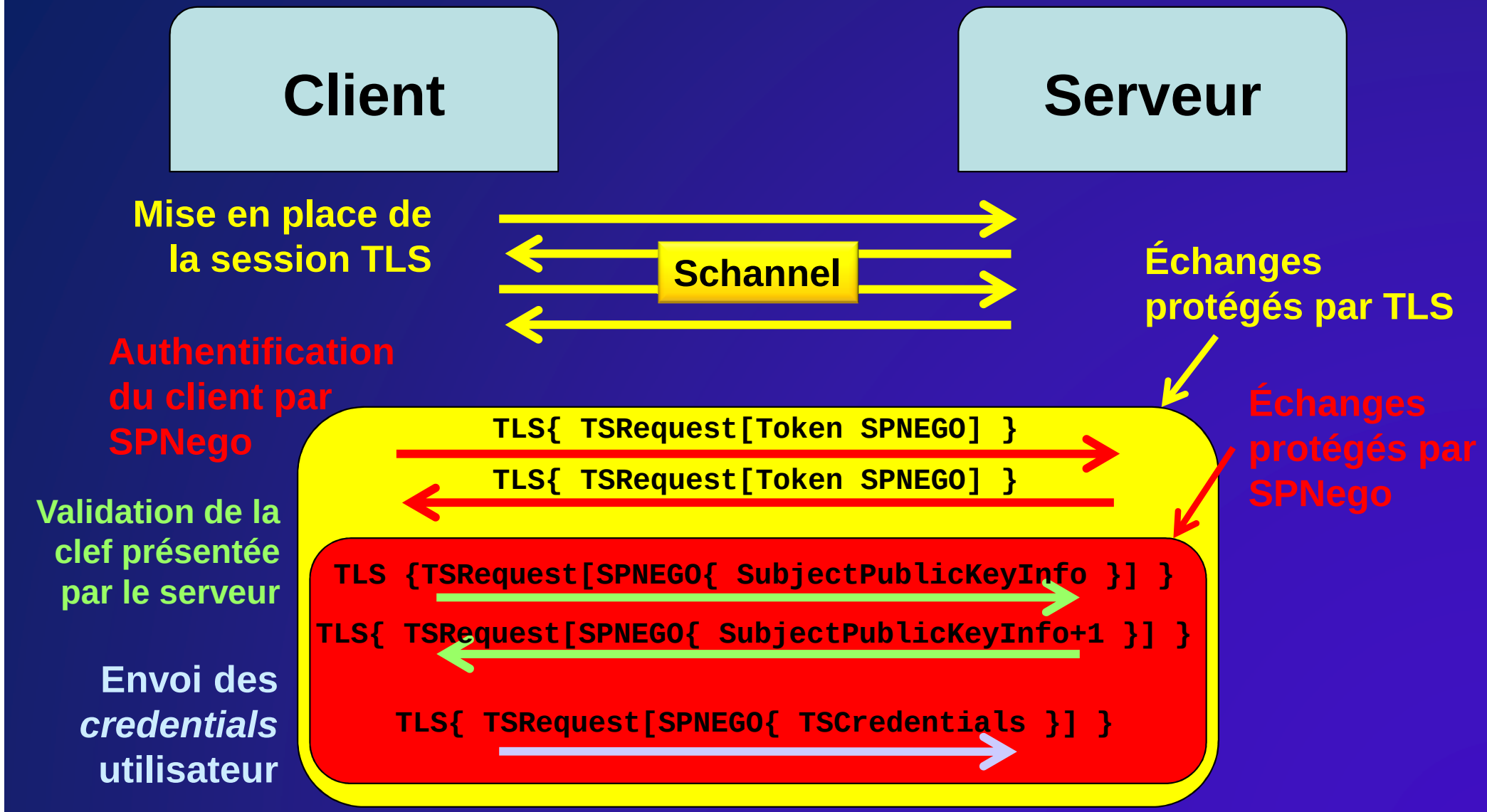
CredSSP

- Implémente le mécanisme d'authentification NLA (*Network Layer Authentication*), dont le principe repose sur :
  - La mise en place d'une session TLS (Schannel)
  - L'authentification du client via SPNego
  - La validation de la clef présentée par le serveur dans son certificat
- Permet la transmission de *credentials* utilisateur (mot de passe ou du code PIN) du client vers le serveur (protégés par TLS + SPNego)

Type de *credentials*

- Trois types de *credentials* peuvent être délégués :
  - *Default credentials* (ceux utilisés pour l'authentification implicite de l'utilisateur courant)
  - *Saved credentials* (*credentials* sauvés)
  - *Fresh credentials* (*credentials* saisis)

Échanges CredSSP



Autorisation de la délégation

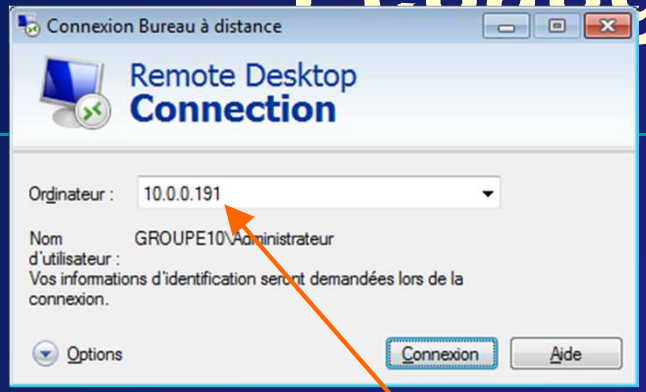
- La délégation doit préalablement être autorisée au travers d'une stratégie de groupe définissant les services et noms des serveurs accrédités
- Stratégie [Ordinateur] :

  Modèles d'administration

  Système

  Délégation d'informations d'identification
- Exemples :
  - TERMSRV/serveur-01.domaine.tld
  - */*

Échanges RDP et CredSSP



mstsc.exe

SSPI

Négo. RDP

Négo. SSP

Messages RDP

Serveur TS

SSPI

TCP/3389

TERMSRV/10.0.0.191

TERMSRV/10.0.0.191

LSASS

Token

Base sessions

Policies CredentialsDelegation

LSASS

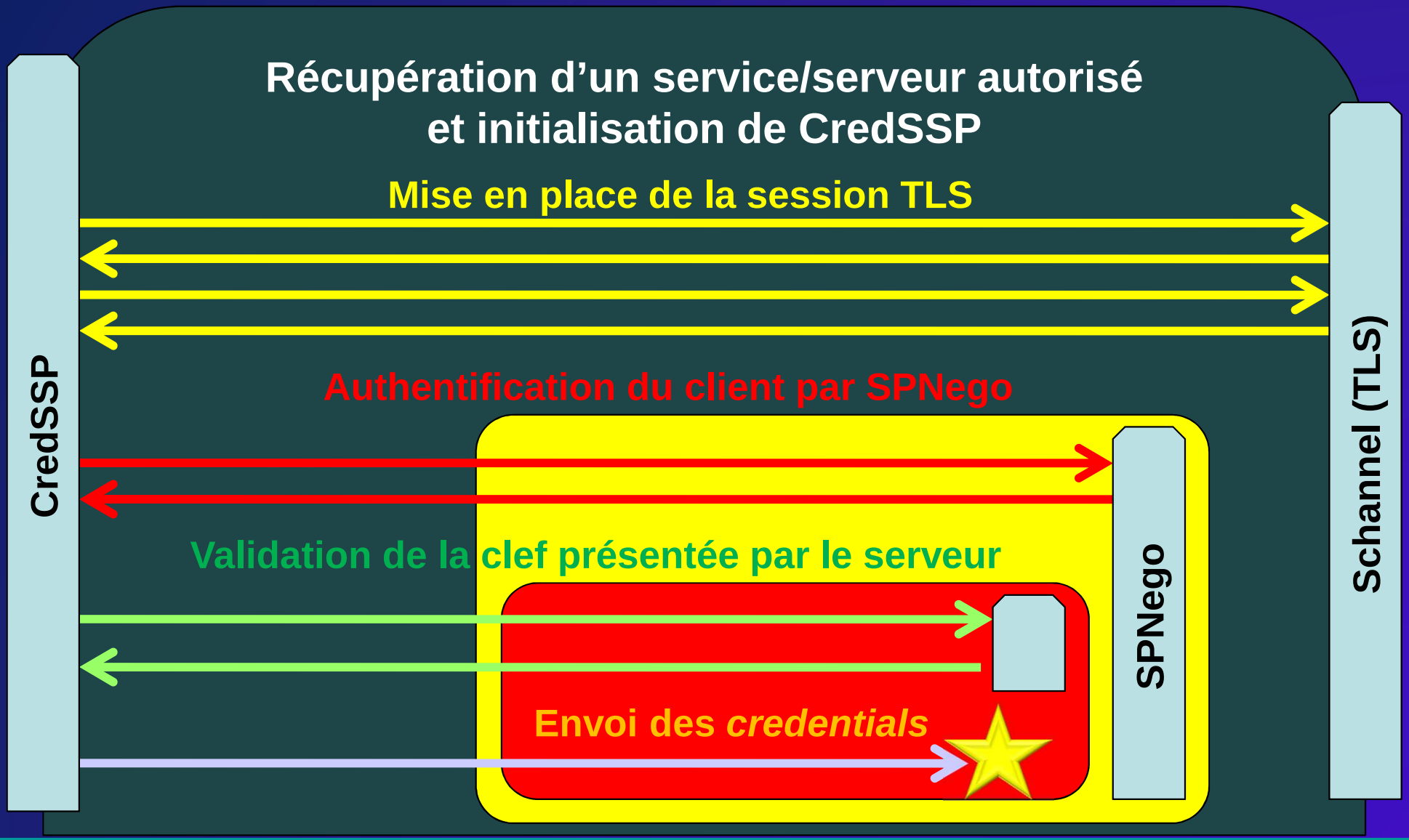
CredSSP

Base sessions

Principe de récupération du bloc `TSCredentials`

- Faire exécuter à un utilisateur un programme qui réalise une authentification via CredSSP du client vers lui-même :
  - La **partie cliente** est une authentification CredSSP à destination d'un serveur autorisé pour la délégation
  - La **partie serveur** est simulée :
    - mise en place de la session TLS
    - authentification SPNEGO du client
    - récupération des *credentials*

Fonctionnement



Recommandation

- la délégation des *credentials* (*default* ou *saved*) doit être utilisée avec la plus grande parcimonie

- L'autorisation d'une seule délégation fait courir au client le risque de compromission de son mot de passe