CredSSP

Aurélien Bordes
aurelien26@free.fr

SSTIC’09 – 4 juin 2009 – Rump sessions

v1.0

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

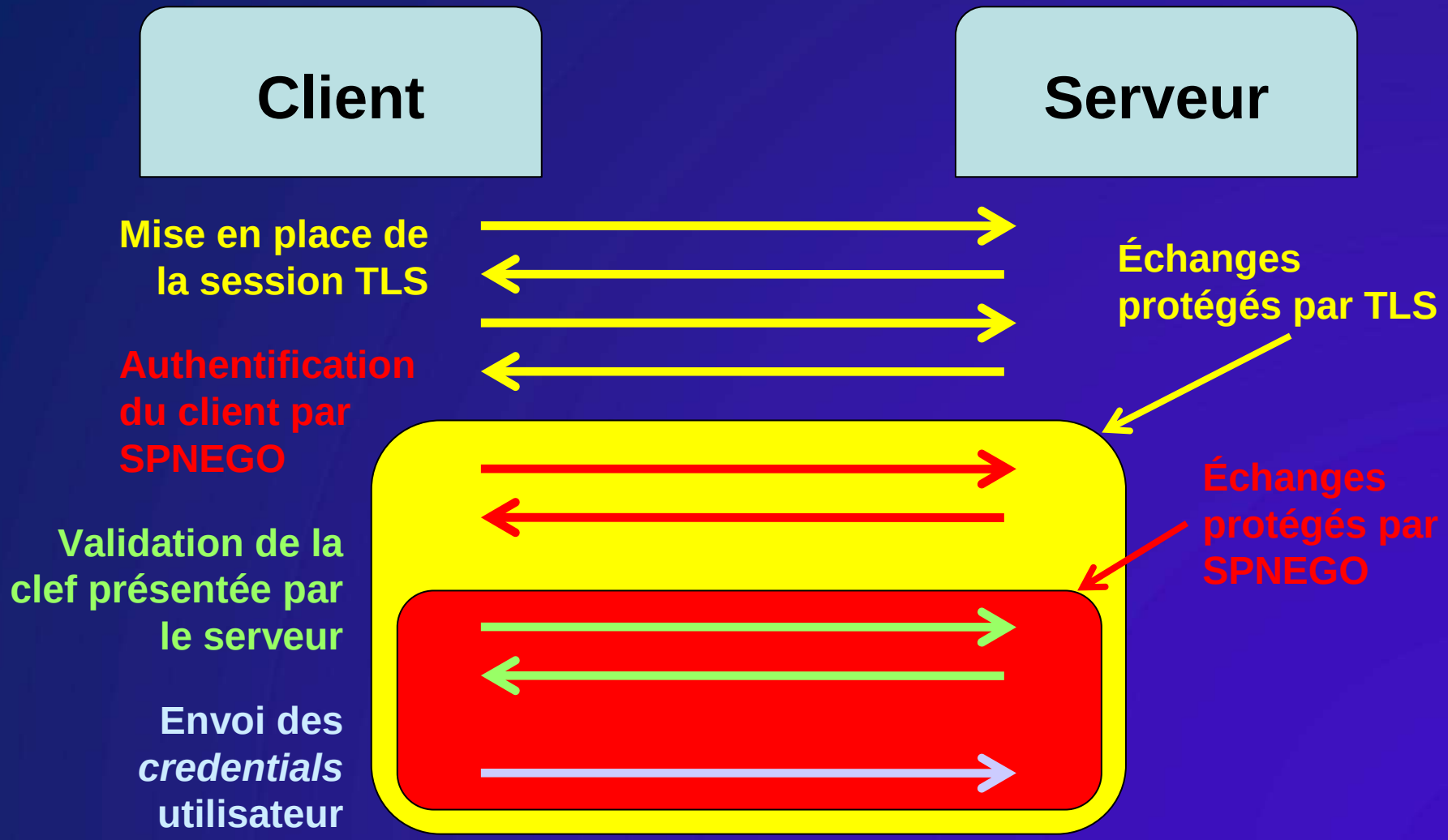
CredSSP

- Implémente le mécanisme d'authentification NLA (*Network Layer Authentication*), dont le principe repose sur :
  - La mise en place d'une session TLS
  - L'authentification du client via SPNEGO
  - La validation de la clef présentée par le serveur dans son certificat
- Permet la transmission des *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 par défaut)
  - *Saved credentials* (sauvés)
  - *Fresh credentials* (nouveaux)

NLA / Délégation



Autorisation de la délégation

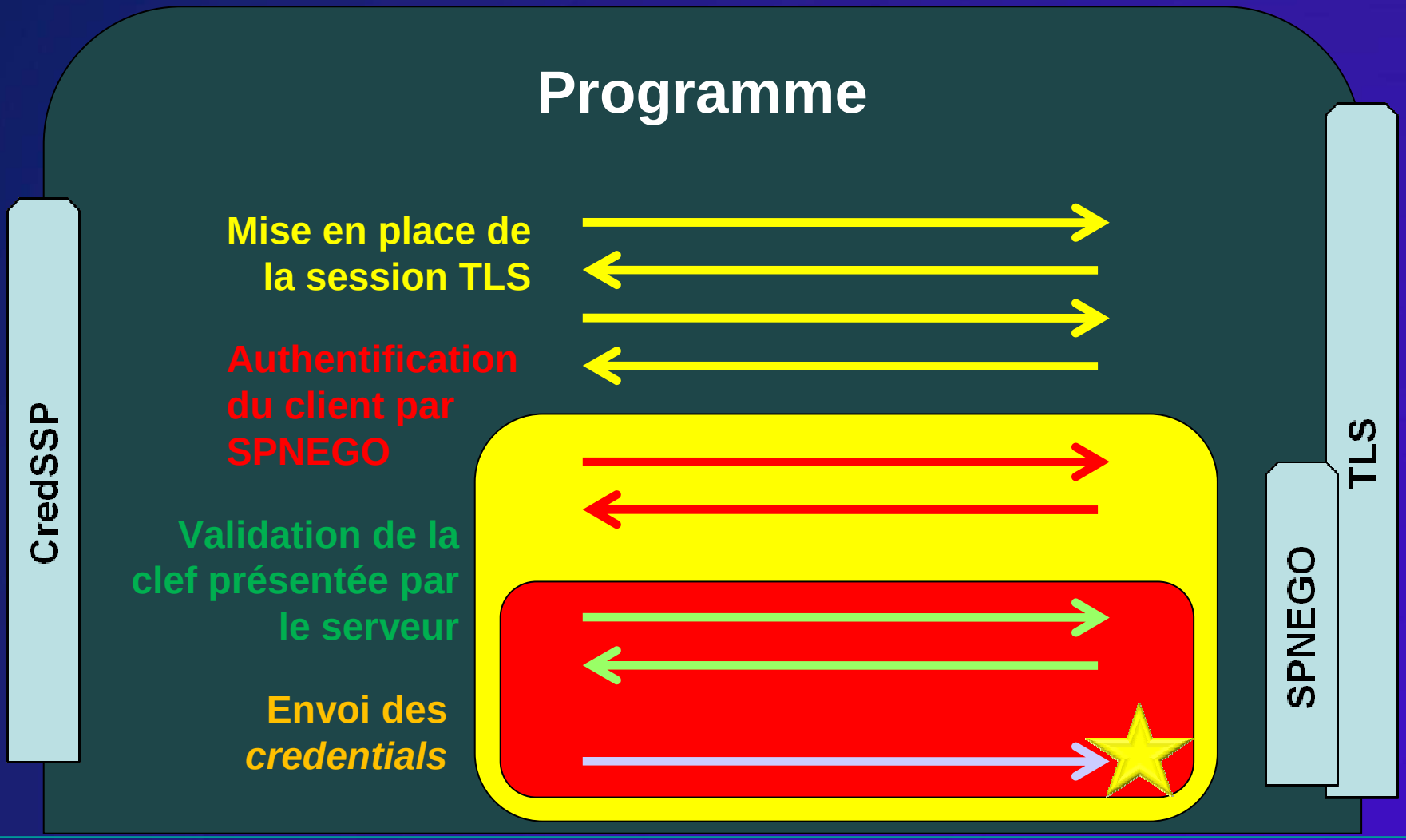
- La délégation doit préalablement être autorisée au travers d'une stratégie de groupe définissant les noms des serveurs accrédités

- Stratégie [Ordinateur] :
  Modèles d'administration
    Système
      Délégation d'informations d'identification

Principe

- 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 cliente 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'un seul serveur fait courir au client le risque de compromission de son mot de passe