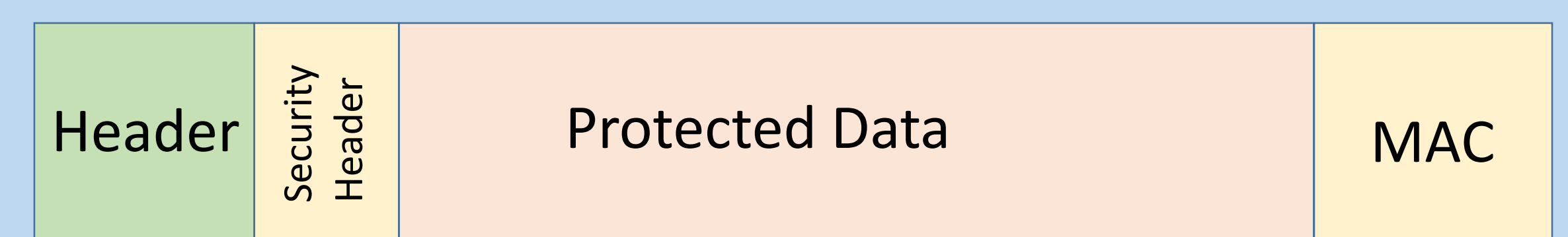
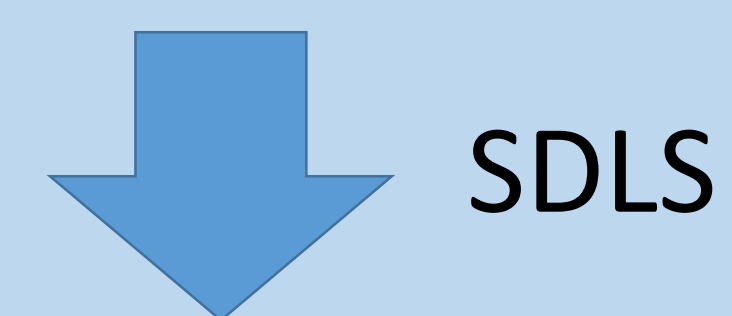
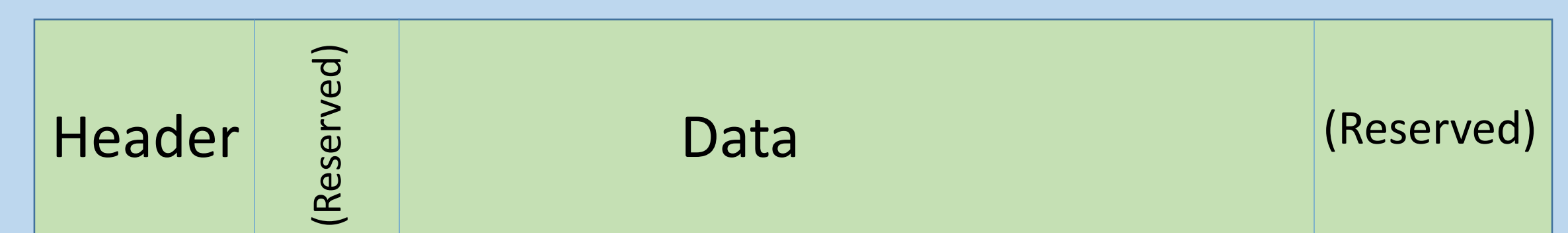


Boîtier Chiffre Sol bas coût

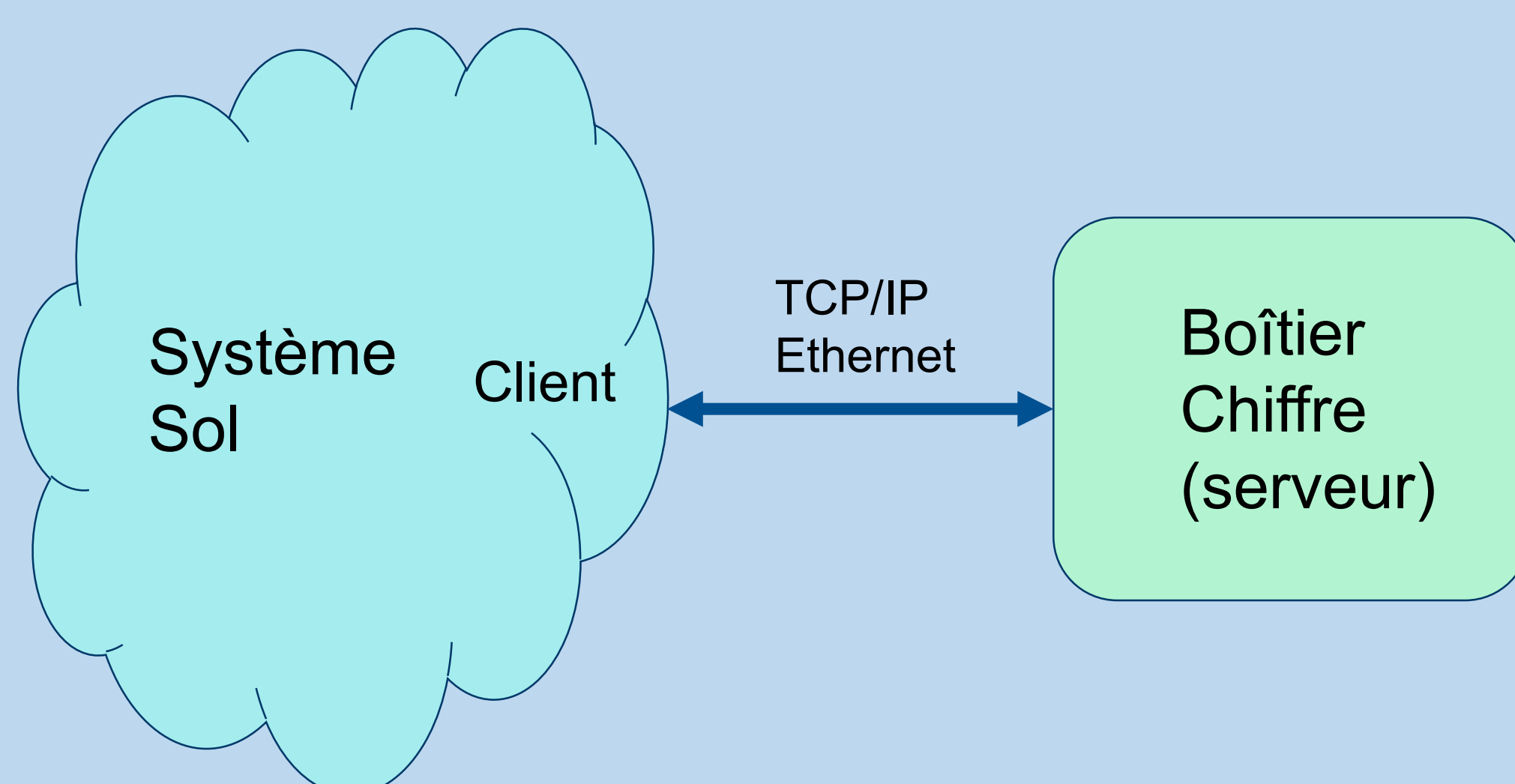
- Authentification / Chiffrement
 - Chiffrement Télécommande
 - Déchiffrement Télémessure
 - Déchiffrement TMCU (AOS)
- Conforme CCSDS / SDLS

Trame CCSDS Initiale



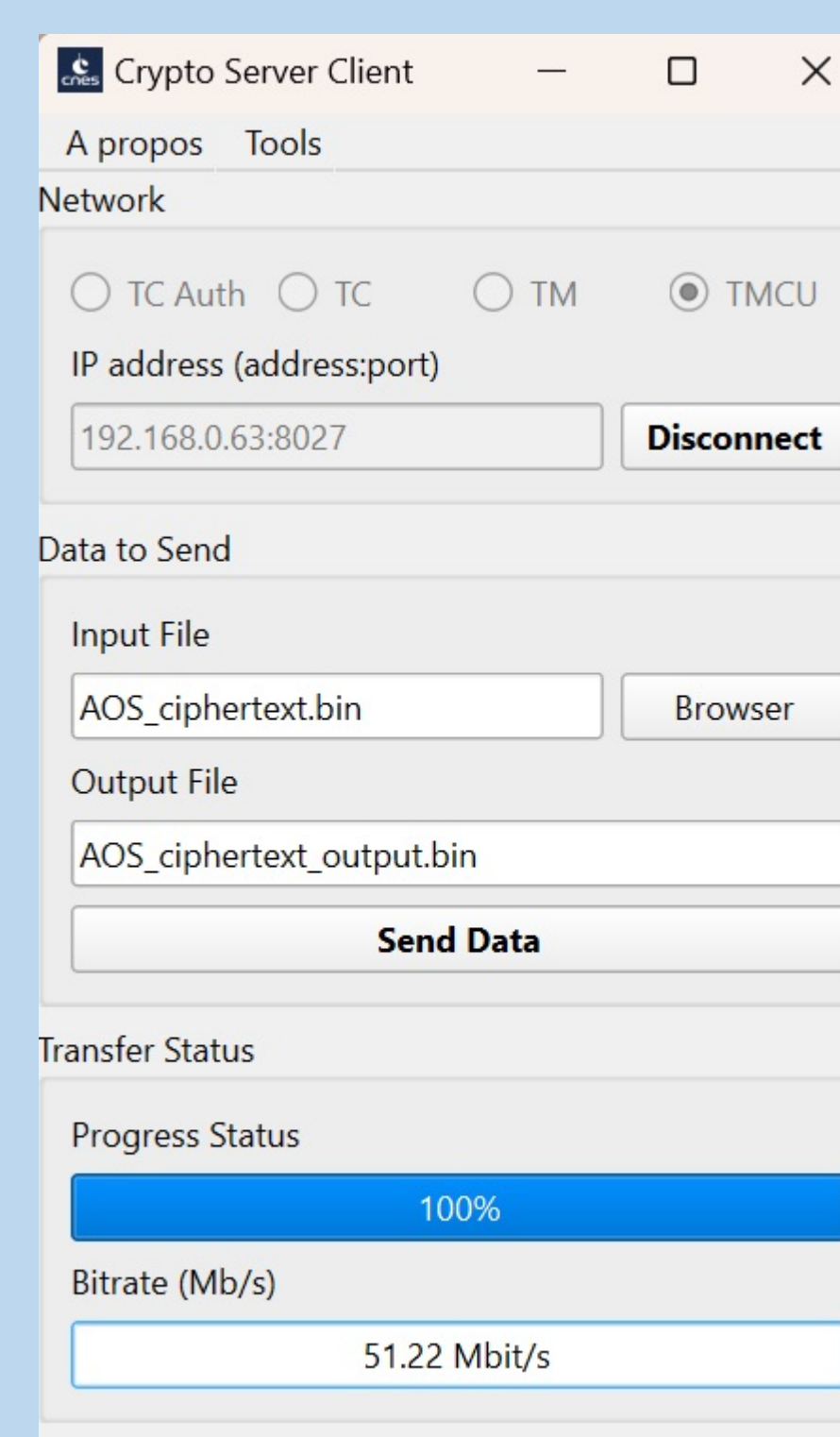
Trame CCSDS protégée

- Intégré au Centre de Contrôle



- Ressource cryptographique
- Coffre-fort de clés
- Interface Ethernet TCP/IP
- Jusqu'à 50 Mbits/s
- AES-256 / GCM ou CMAC
- Basé sur μ C STM32 (STMicro)

- Développement DTN/TVO/ET
- Industrialisé chez BiBench
- Bas coût : 1000 Euros environ
- Ecosystème complet
 - Boîtier Chiffre
 - Générateur de clés
 - Logiciel de gestion de clés
 - Logiciel de test



```

/* (Micro)frame < LastIVused */
{
  ErrorCode = IV_T00_ERR;
  GdFnd = 0; /* Minor error */
  VerbosePrint(VerboseMode, "**** Error IV recu < dernière valeur utilisée
}

/* Test for received IV > Last IV used < IV Window */
else if (((uint32_t) RecvFrameIV < (uint32_t) RecvFnd)
&& ((uint32_t) RecvFrameIV < (uint32_t) (LastIVUsed + IVWindow)))
{
  ErrorCode = IV_T00_ERR;
  GdFnd = 0; /* Minor error */
  VerbosePrint(VerboseMode, "**** Error IV recu > Dernière valeur utilisée +
}

/* Received IV accepted as last IV used */
else
{
  LastIVUsed = RecvFrameIV;
}

/* Last IV used == Buff... */
if (LastIVUsed == 0x00000000 && (ErrorCode == 0)) /* Buffer full */
{
  ErrorCode = IV_T00_ERR;
  GdFnd = 0; /* Minor error */
}
  
```