Re-Trust meeting - Session 3

d'Annoville Jerome
Project Manager

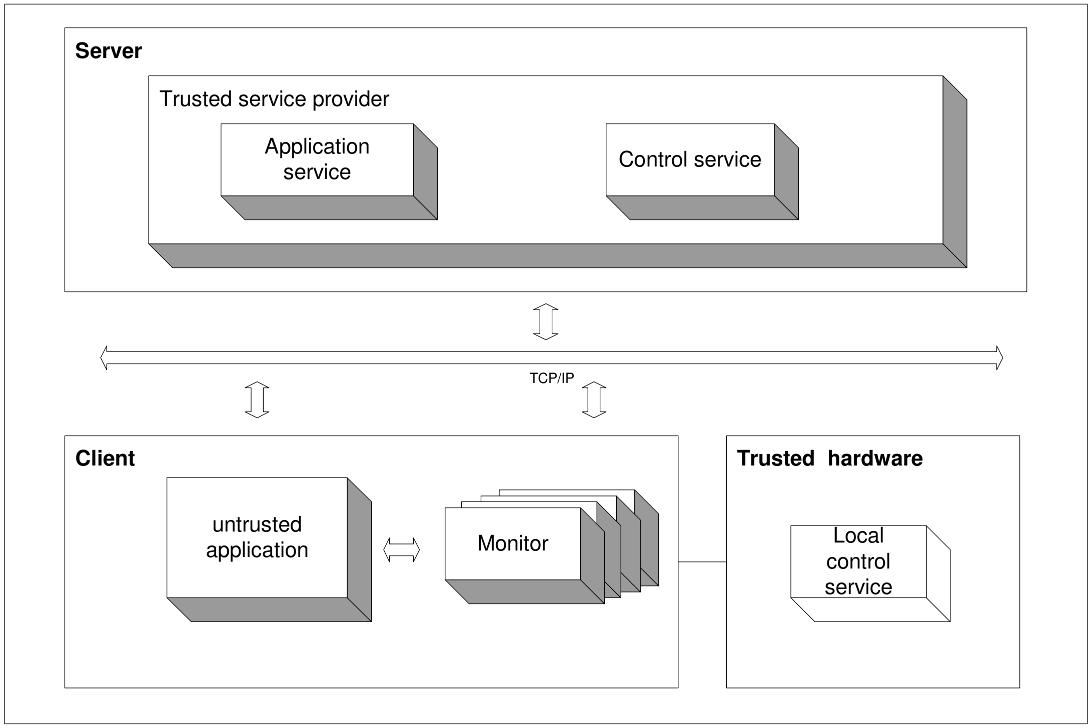
03/21/07

Session 3 - Design Alternatives

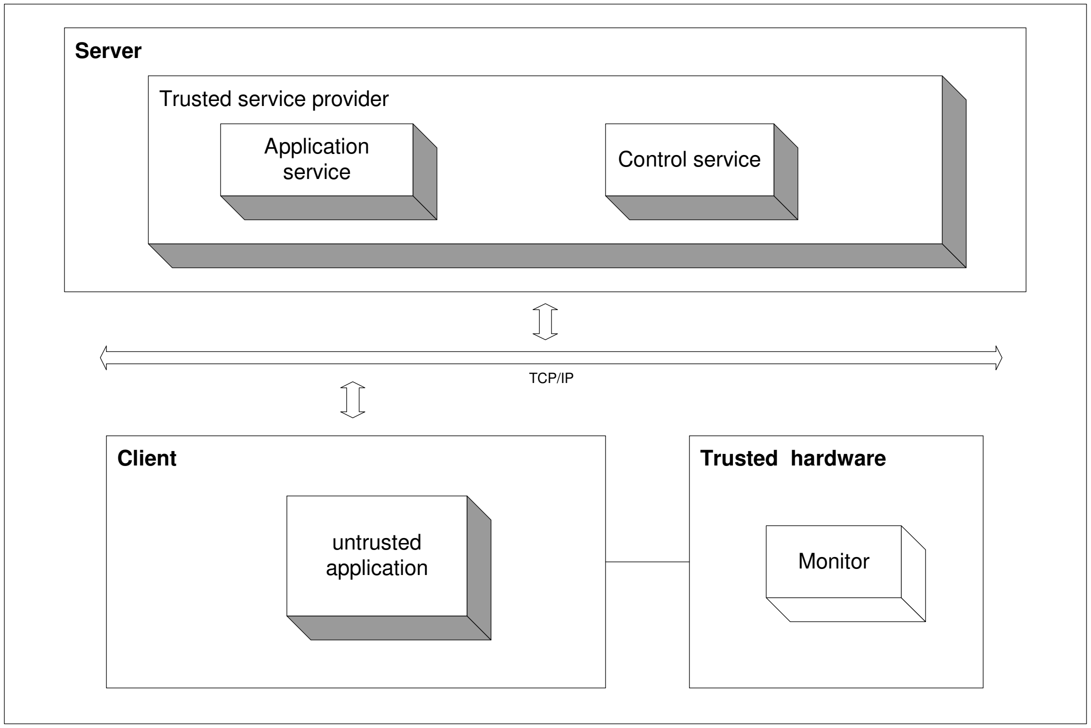
Available technologies

- Dongle
- TPM
- Smartcard
- Hardware Security Module (HSM)
- Secure coprocessor
- (USB token)

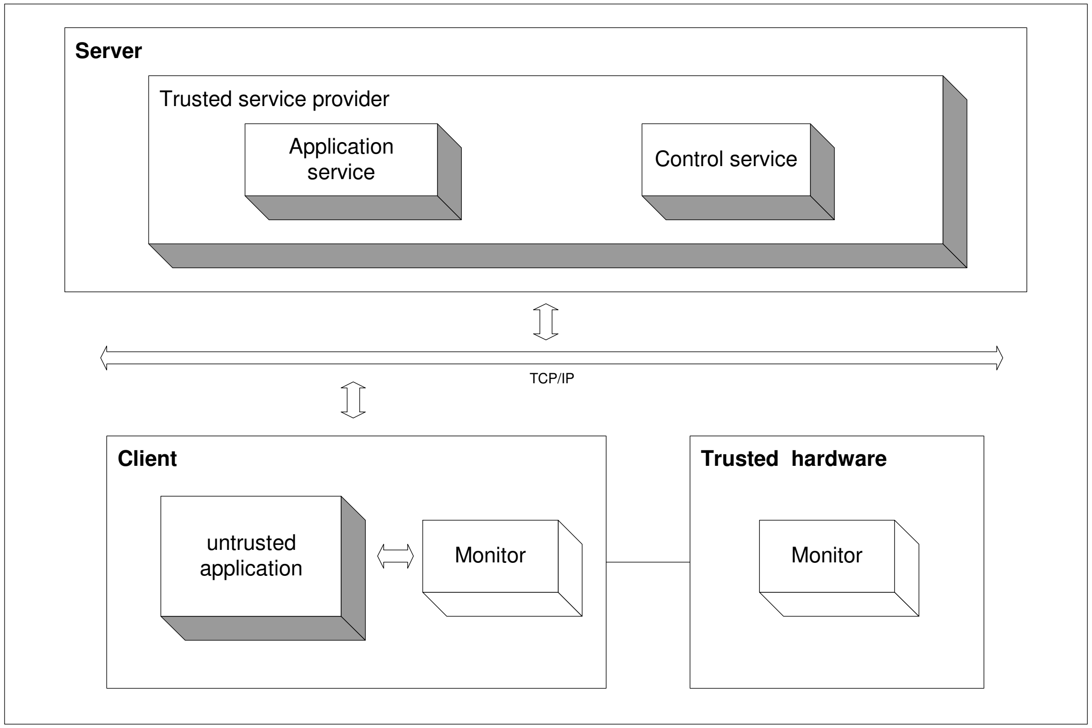
Server split



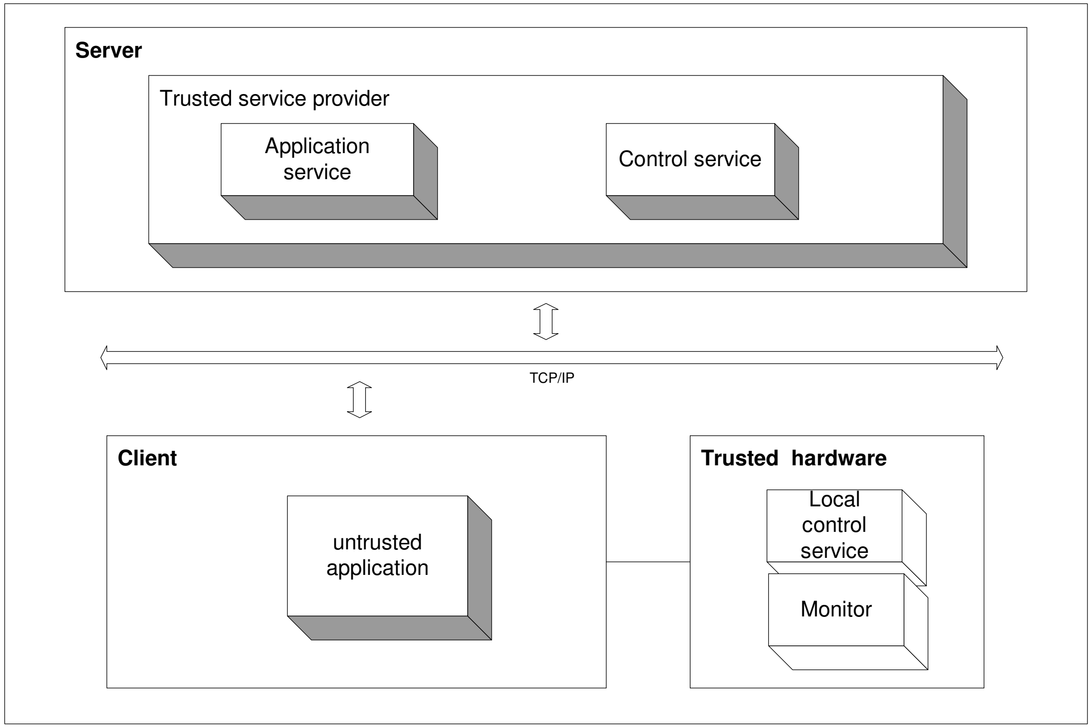
Trusted monitor (1/2)



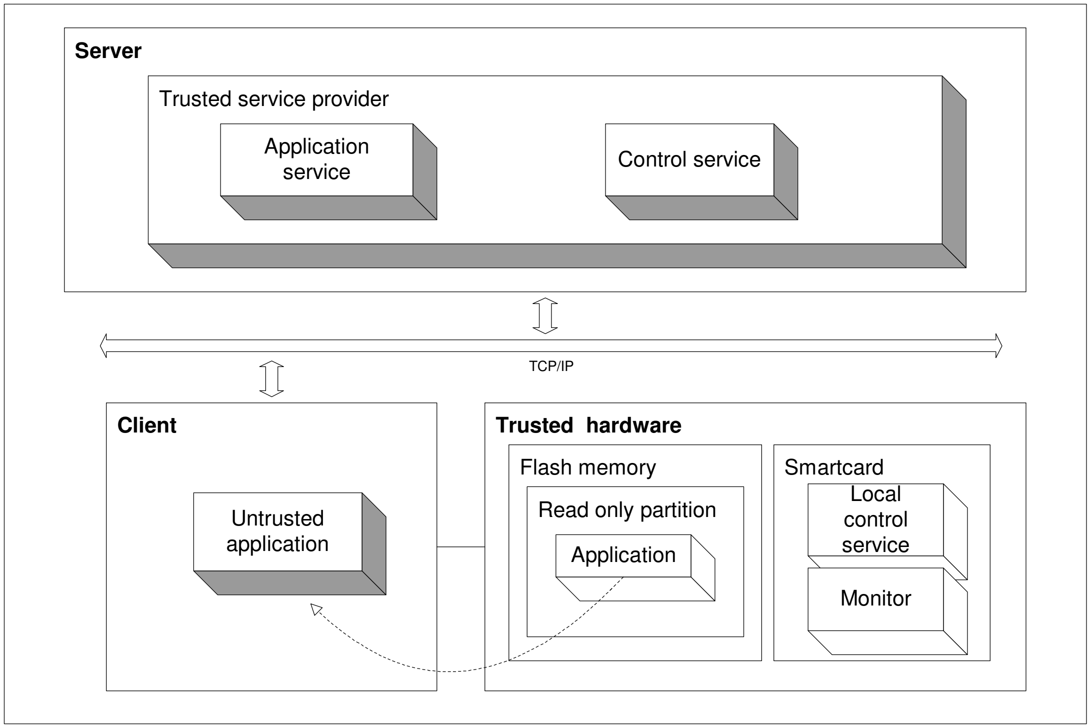
Trusted monitor (2/2)



Trusted monitor and server split



“Safe” application


Server
Trusted service provider
Application service
Control service
TCP/IP
Client
Untrusted application
Trusted hardware
Flash memory
Read only partition
Application
Smartcard
Local control service
Monitor