Windows 2000 Identification

Mario Pasquali

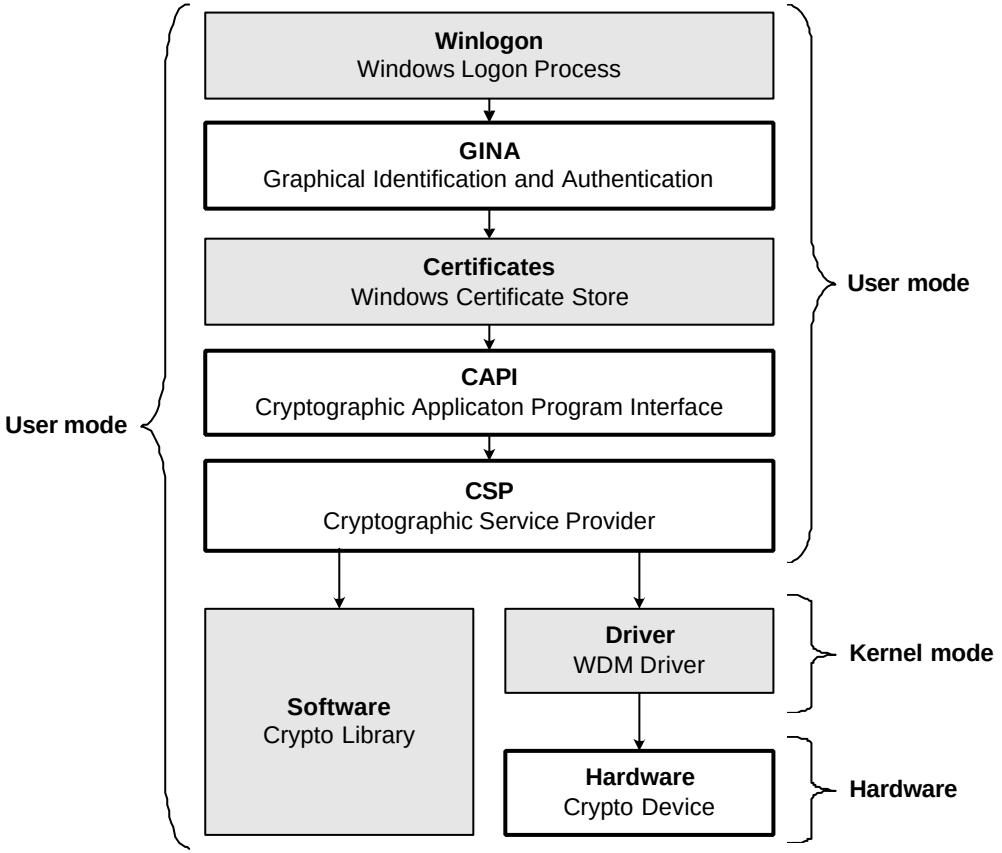
13 décembre 2001

En collaboration avec: ellisys

Vue d'ensemble

- Thèmes traités
  - Windows Smart Card Logon
  - Développement d'une DLL GINA
  - Développement d'un CSP CryptoAPI

Vue d'ensemble (2)



Windows 2000 Identification

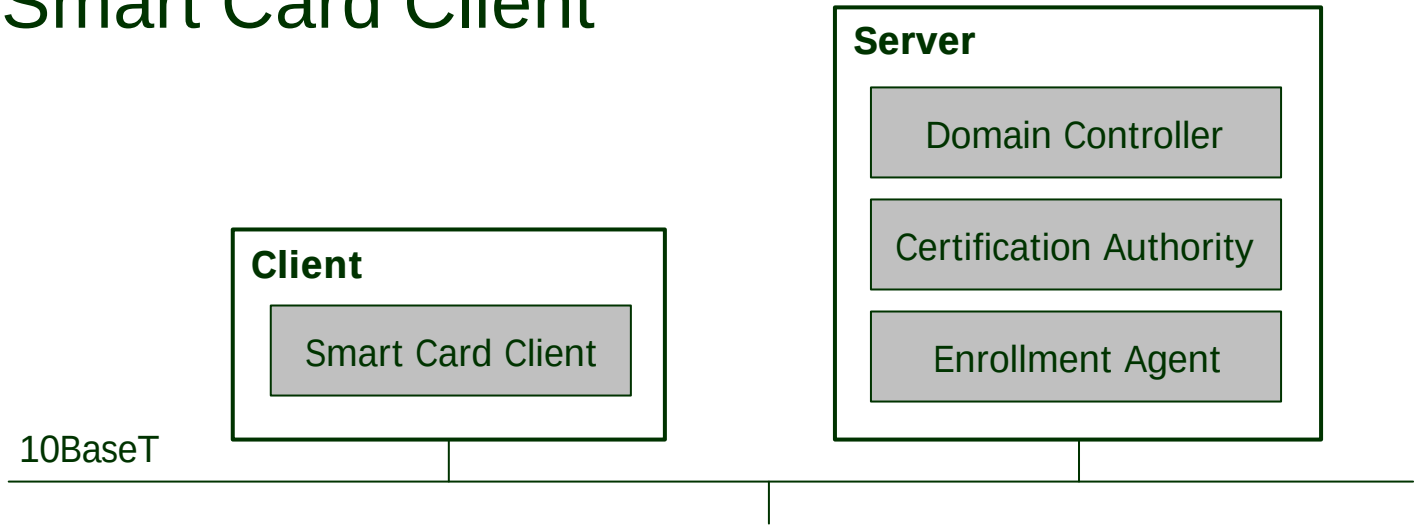
Windows
Smart Card Logon

Introduction

- Infrastructure à clé publique (PKI)
- Cartes à puces
- Mise en œuvre avec eToken d'Aladdin

Configuration

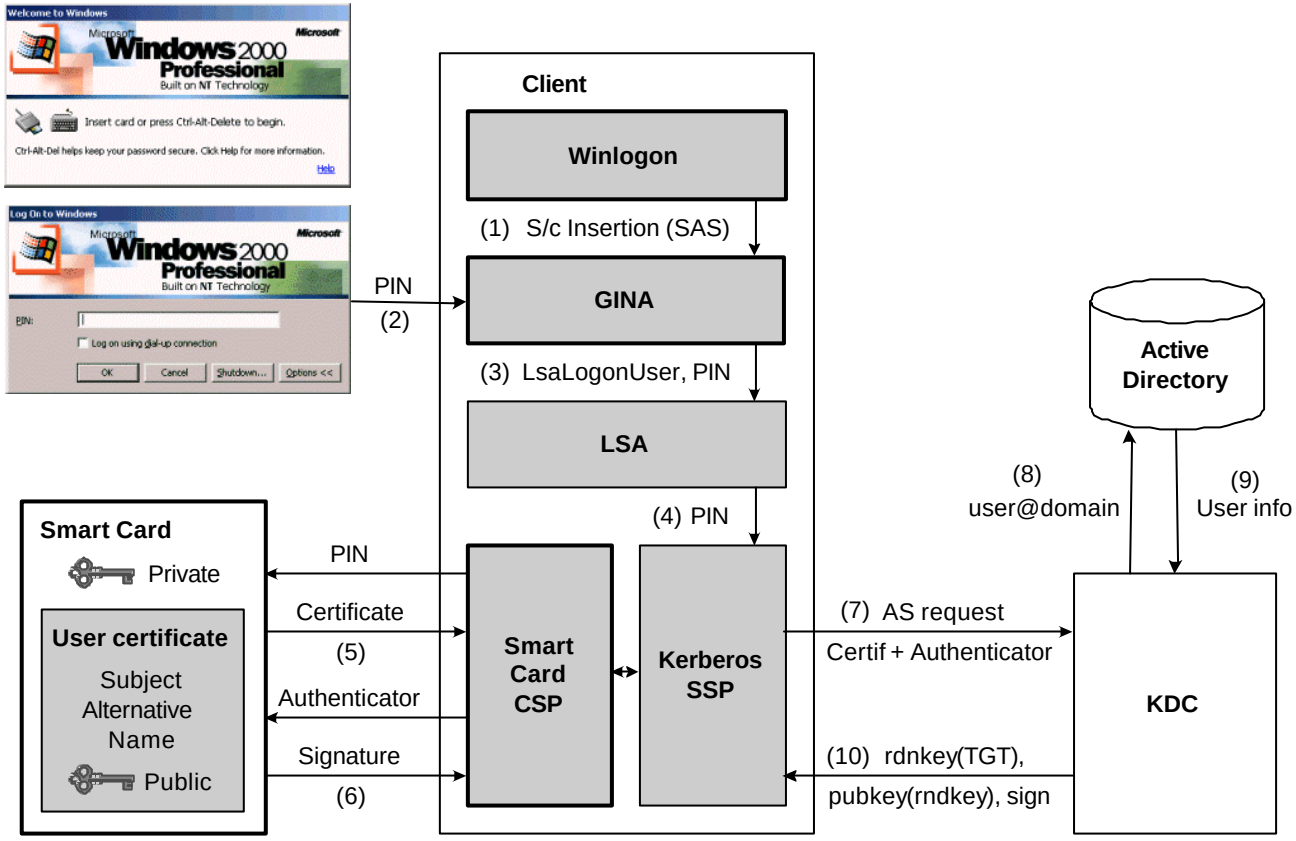
- Windows 2000 domain controller
- Certificate Authority
- Smart Card Enrollment Agent
- Smart Card Client



Kerberos

- Protocole d’authentification
- Supporté par Windows 2000
- Phase d’initialisation avec clés symétriques

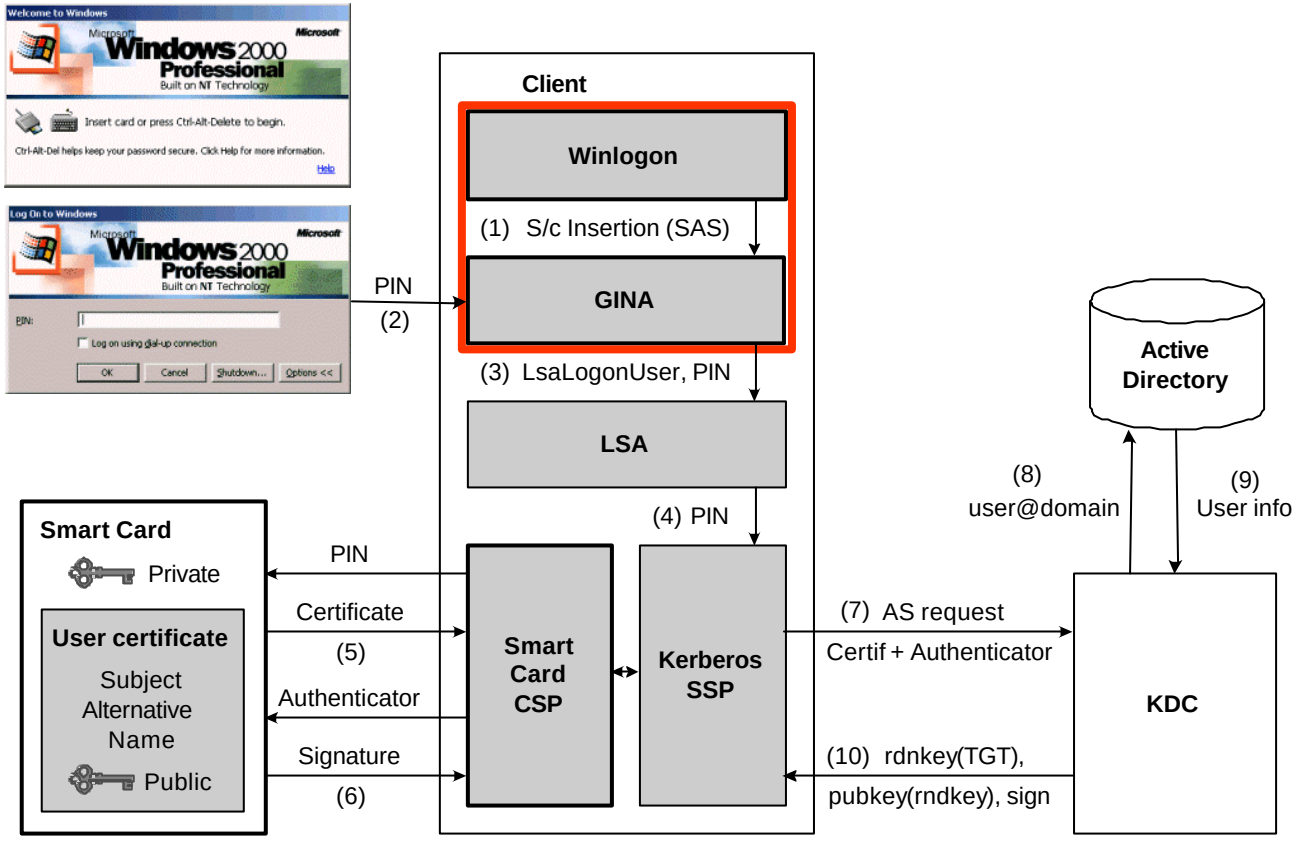
Extension PKINIT de Kerberos



Windows 2000 Identification

Introduction à Winlogon et GINA

Contexte


Welcome to Windows
Windows 2000 Professional
Built on NT Technology
Insert card or press Ctrl-Alt-Delete to begin.
Ctrl-Alt-Del helps keep your password secure. Click Help for more information.
Help
Log On to Windows
Windows 2000 Professional
Built on NT Technology
PIN:
Log on using dial-up connection
OK
Cancel
Shutdown...
Options <<
PIN
(2)
Client
Winlogon
(1) S/c Insertion (SAS)
GINA
(3) LsaLogonUser, PIN
LSA
(4) PIN
Smart Card
Private
User certificate
Subject Alternative Name
Public
PIN
Certificate
(5)
Authenticator
Signature
(6)
Smart Card CSP
Kerberos SSP
(7) AS request
Certif + Authenticator
(10) rdnkey(TGT), pubkey(rndkey), sign
Active Directory
(8) user@domain
(9) User info
KDC

Composants de Winlogon

- Winlogon.exe
  - Premier processus exécuté par le système d'exploitation
- GINA
  - Identification et authentification graphique
  - Gère l'intéraction avec l'utilisateur

- Network Providers
  - Donnent accès à divers types de réseaux

Winlogon et GINA

- Tâches de Winlogon
  - Enregistrement de ‘Ctrl-Alt-Del’
  - Création des ‘bureaux’ (desktops)
  - Appel des points d’entrée de GINA
- Tâches de GINA
  - Reconnaissance des SAS spécifiques
  - Authentification de l’utilisateur
  - Création du shell utilisateur

Windows 2000 Identification

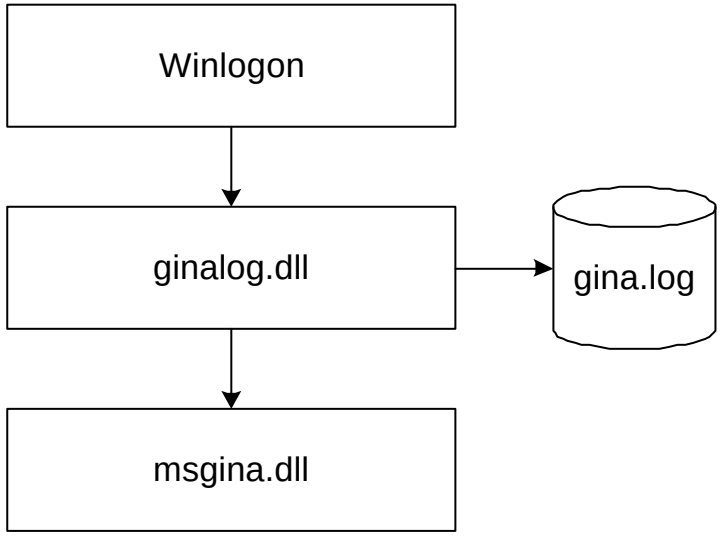
Développement d’une DLL GINA

Objectifs

- Authentification d'un utilisateur dans le domaine local d'une station de travail
- Interfaçage avec du matériel spécifique

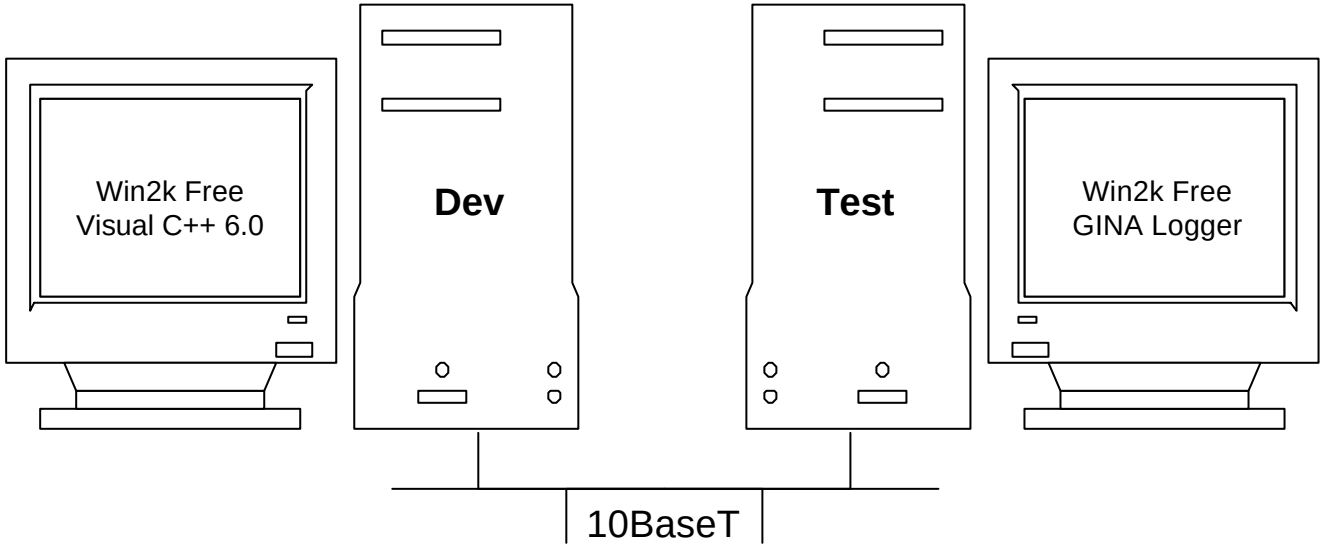
DLL de traçage

- Expérience avec GINA
- Compréhension des points d'entrée
- Principe



Environnement de test

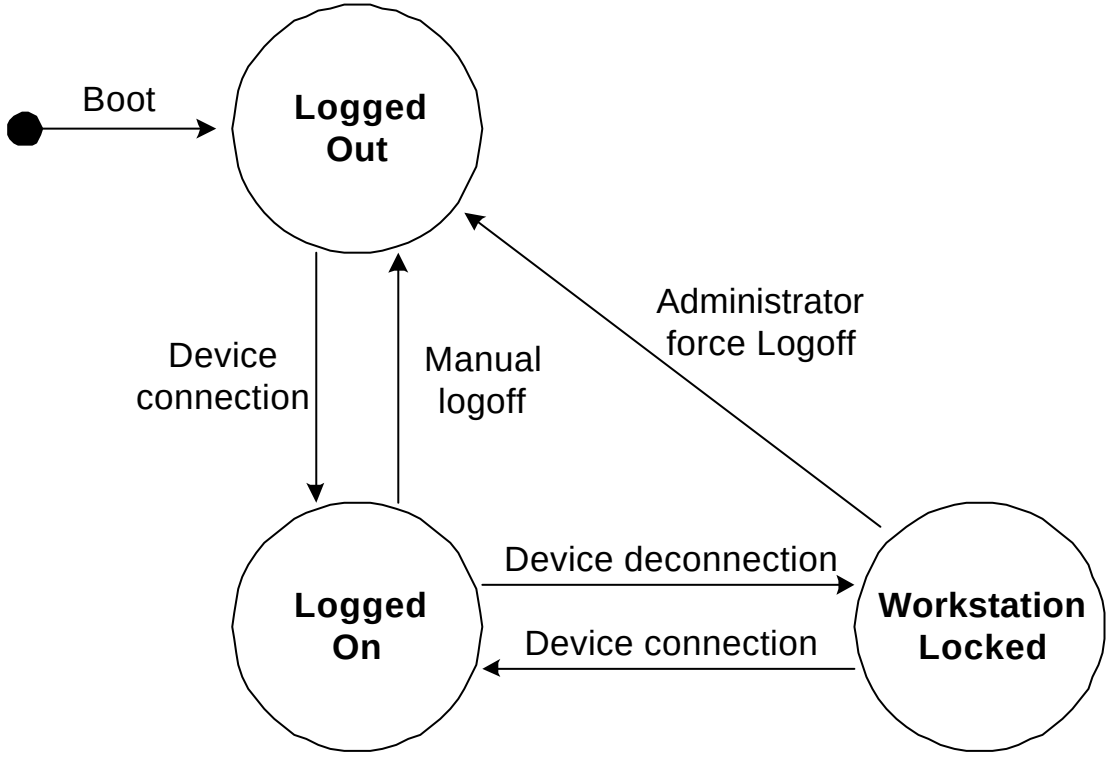
- Utilisation d'un log



Interfaçage avec matériel spécifique

- Carte de développement USB
- Informations de logon stockées en mémoire non-volatile de la carte USB
- SAS spécifiques
  - Insertion de la carte USB
  - Extraction de la carte USB

Interfaçage avec matériel spécifique (2)



Interfaçage avec matériel spécifique (3)

- Démonstration (3 min)

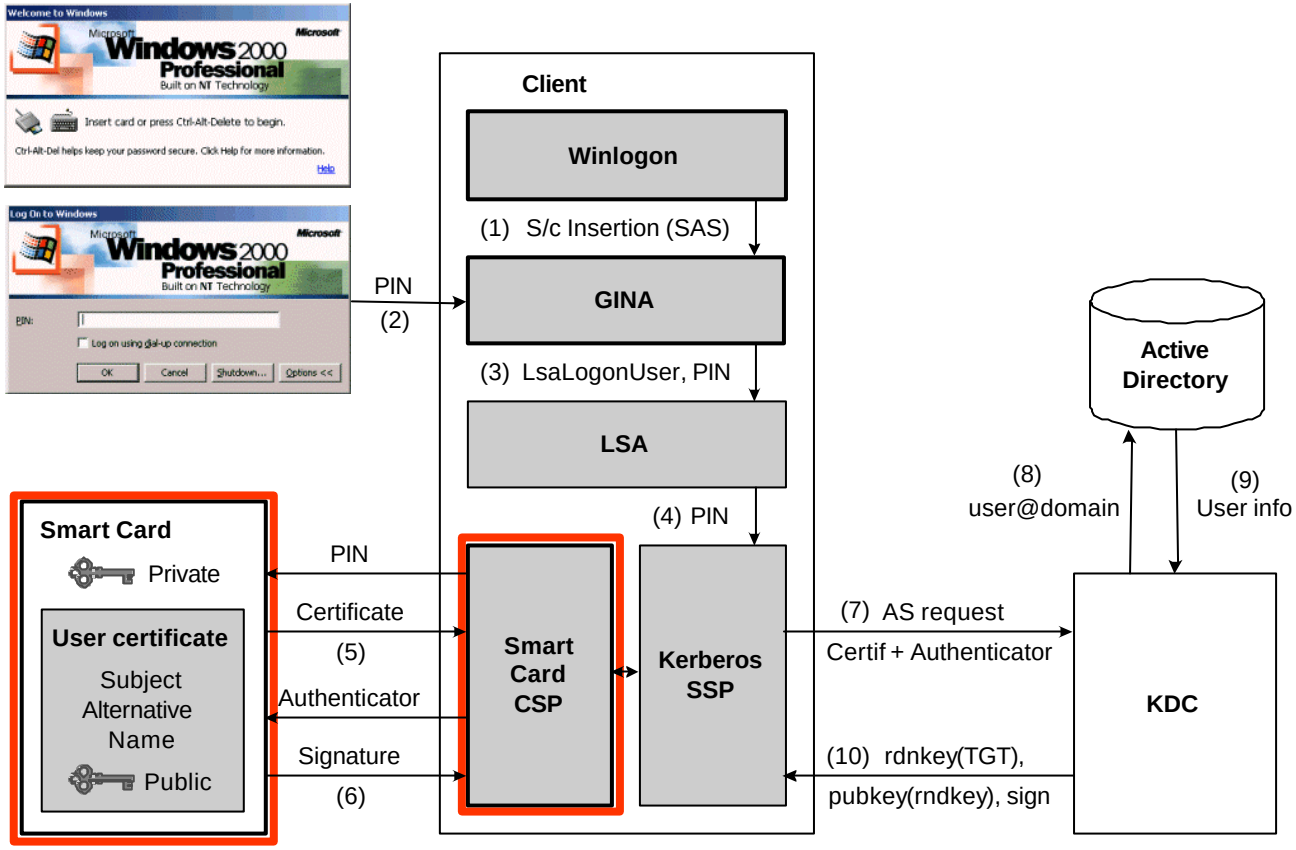
Conclusion

- Redémarrages fréquents
- Machine de test performante conseillée

Windows 2000 Identification

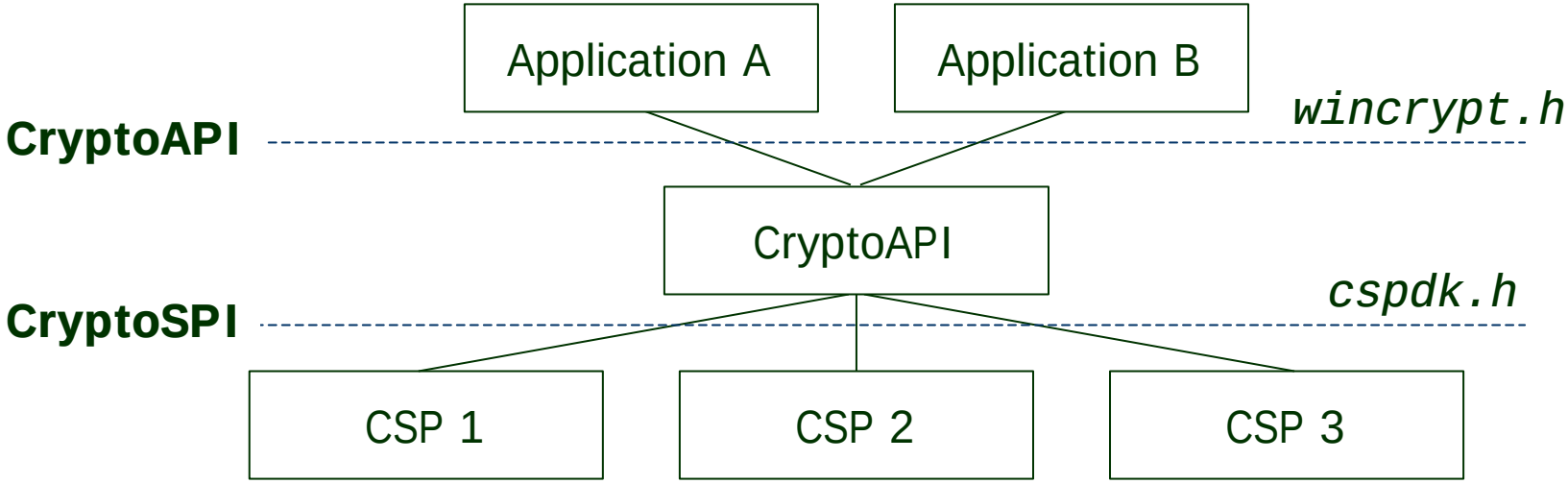
Introduction à CryptoAPI

Contexte


Welcome to Windows
Windows 2000 Professional
Built on NT Technology
Insert card or press Ctrl-Alt-Delete to begin.
Ctrl-Alt-Del helps keep your password secure. Click Help for more information.
Help
Log On to Windows
Windows 2000 Professional
Built on NT Technology
PIN:
Log on using dial-up connection
OK
Cancel
Shutdown...
Options <<
PIN
(2)
Client
Winlogon
(1) S/c Insertion (SAS)
GINA
(3) LsaLogonUser, PIN
LSA
(4) PIN
Smart Card
Private
User certificate
Subject
Alternative
Name
Public
PIN
Certificate
(5)
Authenticator
Signature
(6)
Smart Card CSP
Kerberos SSP
(7) AS request
Certif + Authenticator
(10) rdnkey(TGT),
pubkey(rndkey), sign
Active Directory
(8)
user@domain
(9)
User info
KDC

CryptoAPI

- Jeu de fonctions cryptographiques
- Applications indépendantes du matériel



CSP (Cryptographic Service Provider)

- Fournisseur de services cryptographiques
- Diverses implémentations
  - Hardware
  - Software
  - Mixed

Windows 2000 Identification

Développement d’un CSP CryptoAPI

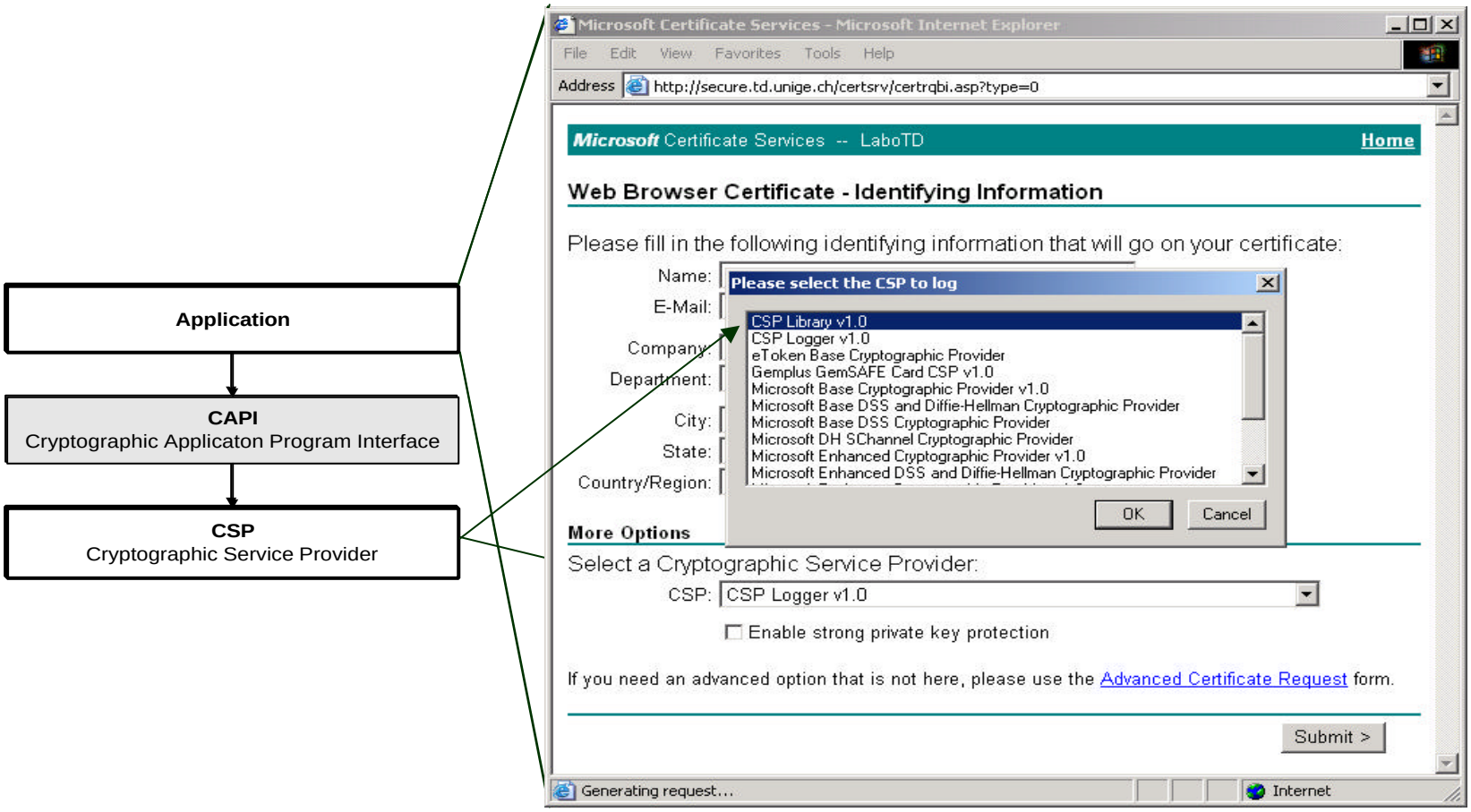
Objectifs

- Génération d’un certificat
- Opérations cryptographiques en logiciel avec une librairie cryptographique

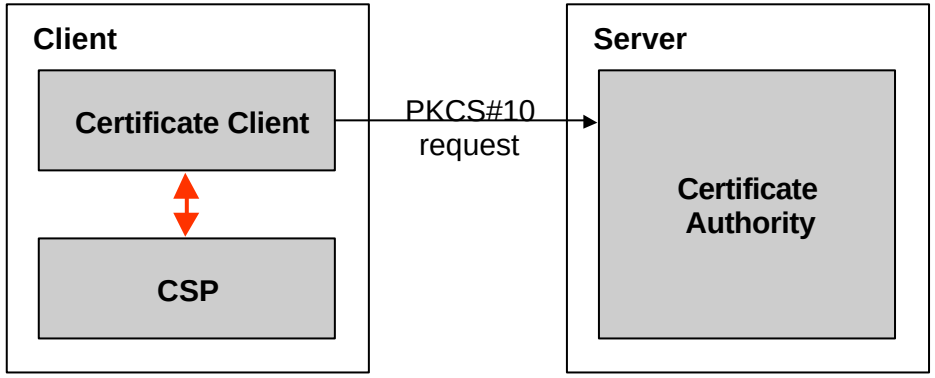
Déroulement du développement

- Développement d’un squelette
- Trace de la génération d’un certificat
- Développement des fonctions utilisées
- Validation des fonctions écrites

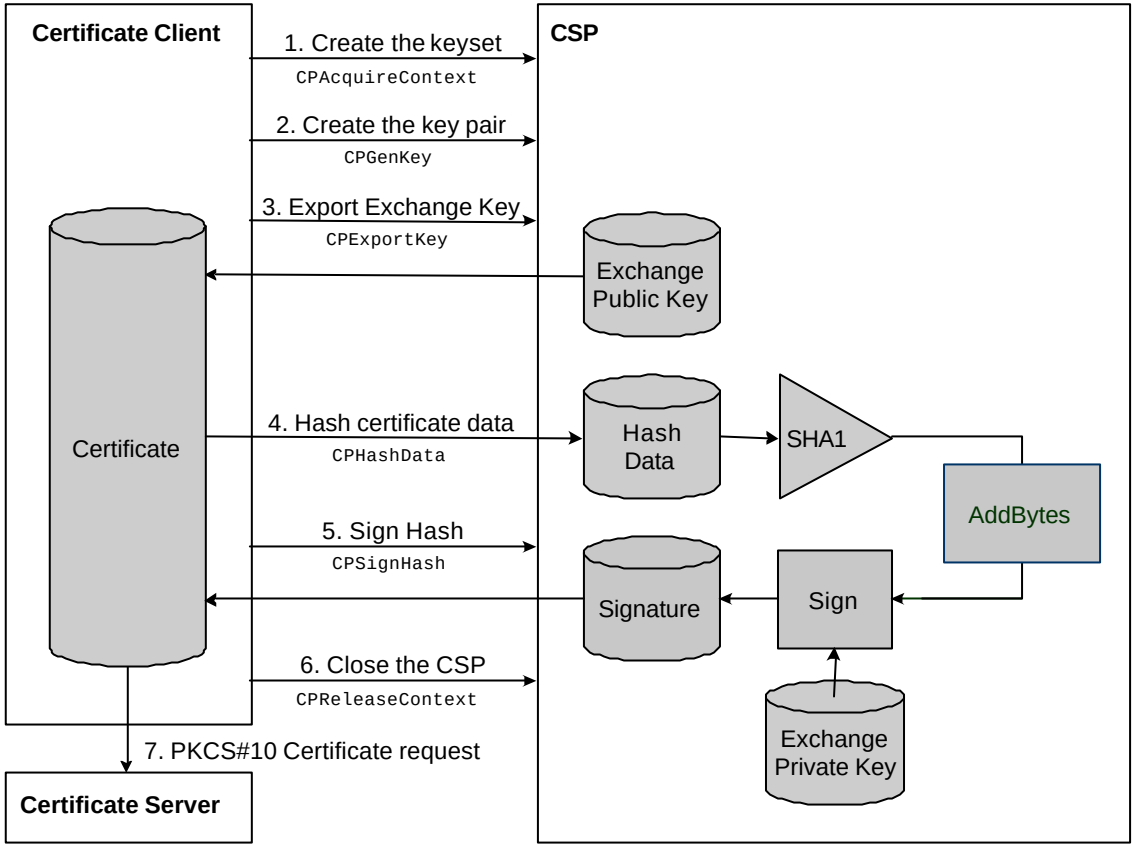
CSP de traçage



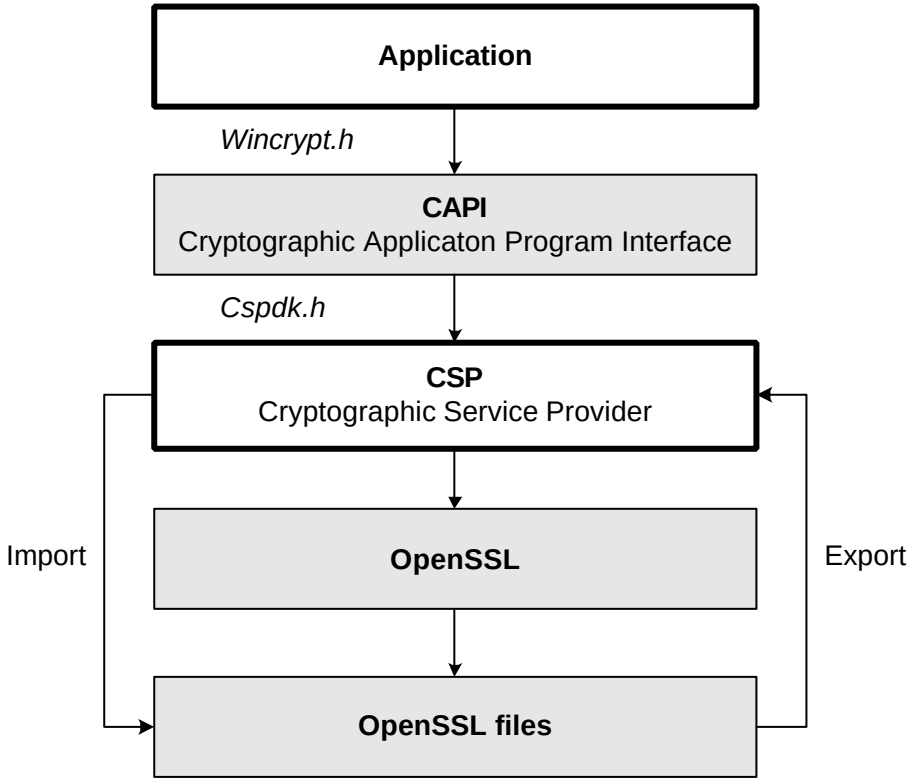
Requête de certificat



Requête d'un certificat (2)



Implémentation avec OpenSSL



Implémentation avec OpenSSL

- Démonstration (7 min)

Conclusion

- Beaucoup de code nécessaire avant de commencer réellement
- Manque de ressources (documentation, code source, exemples)
- Futur travail grandement simplifié

Temps passé sur chaques parties

- Smart Card Logon = 1 semaine
- GINA = 3 semaines
  - GinaLog = ½ semaine
  - GinaLib = 1 ½ semaines
  - UsbGina = 1 semaine (1’500 lignes de code)
- CSP = 7 semaines
  - CspLog = 1 ½ semaines (1’300 lignes de code)
  - Framework = 3 semaines (2’500 lignes de code)
  - Crypto++ = ½ semaine
  - OpenSSL = 1 semaine (framework + 500 lignes de code)
  - Problème format = 1 semaine

Windows 2000 Identification

Questions (10 min)