



# NCS AUTHENTICATION SOLUTION

NCS Solutions Corporation  
No 5, 535 Alley, Kim Ma Street, Ba Dinh, Hanoi, Vietnam  
Tel: (84-4) 7164181  
Fax: (84-4) 7164287  
E-mail: [info@ncs.com.vn](mailto:info@ncs.com.vn)  
Tech support: [techsupport@ncs.com.vn](mailto:techsupport@ncs.com.vn)  
URL: <http://www.ncs.com.vn>

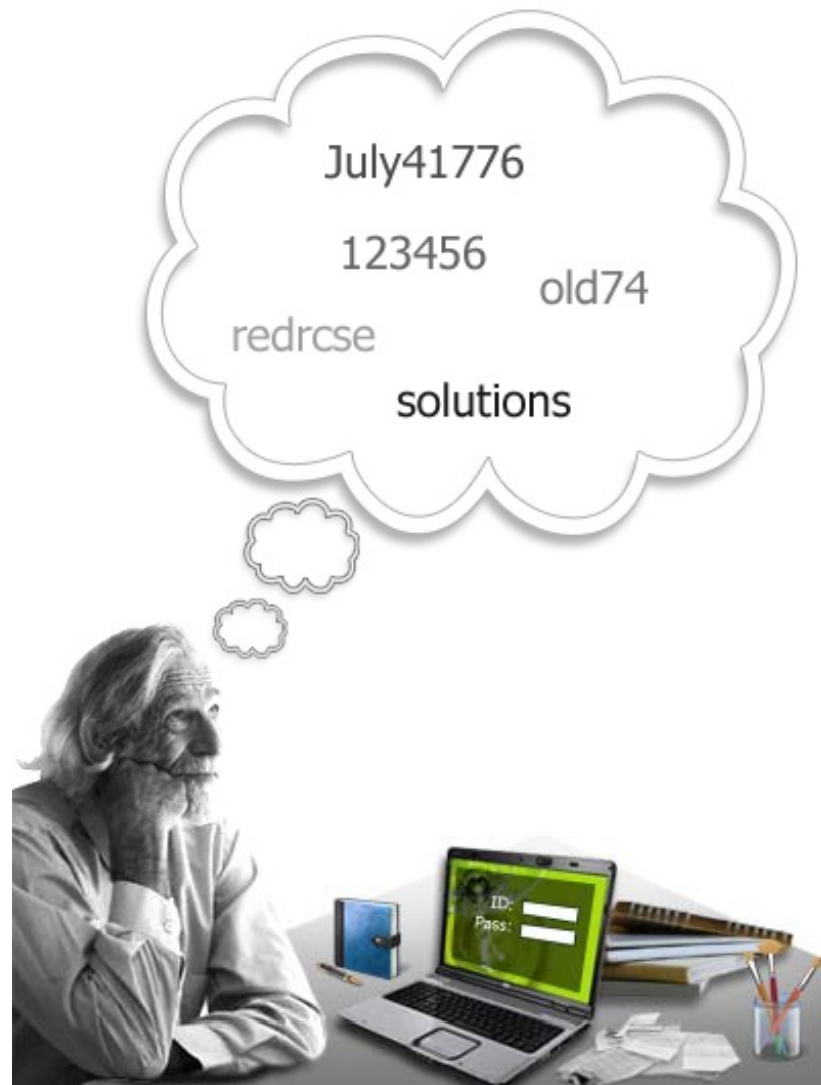
# Agenda



- Authentication technology
- Issues with Password Authentication
- PKI Authentication
- NCS Solution
- Integrated component
- Certificate Management

# Issues with Password authentication

- Too many for them to manage
- Passwords easily shared with others (in violation of access policy)
- Easily captured over a network if no encrypted channel used
- Weak passwords can be guessed or brute forced offline



# Issues with Password authentication



- Vulnerable to keyboard sniffing/logging attacks on public or compromised systems
- Cannot provide non-repudiation since they generally require that the user be enrolled at the service provider, and so the service provider also knows the user's password
- Vulnerable to Social Engineering attacks
- Vulnerable to dictionary attacks even if encrypted channels are used
- Single factor of Authentication only

# PKI authentication



- Solution to Password vulnerabilities based on [Public Key Infrastructure \(PKI\)](#)
  - End users have a key pair – 1 public, stored in a certificate, 1 private, stored in a protected file or smartcard
  - Allows exchange of session secrets in a protected (encrypted) manner without disclosing private key
  - PKI lets users authenticate without giving their passwords away to the service that needs to authenticate them

# Advantages of PKI authentication



- Eliminate user passwords on network servers
- PKI credentials are local in the application key store or in hardware token
- User manages the password and only has one per set of credentials
- Still need process for forgotten password, but it is only one for all applications using PKI authentication, and users are much less likely to forgot it since they use it frequently and control it themselves.

# PKI Provides two factor authentication



1. Something the user has(Credentials stored in the application or smartcard or token)
  2. Something the user knows(password or unlock credentials)
- Significant security improvement, especially with smartcard or token
  - Reduce exposure to password sharing(token is difficult to share)

# Digital Signatures

- PKI enables digital signatures
  - Improved assurance of electronic transactions
  - Recognized by Federal Government as legal signatures
  - Reduce paperwork via electronic form
  - Faster, more traceable business processes

A handwritten signature in black ink that reads "Nassolutions". The signature is written in a cursive, flowing style with a long, sweeping tail that extends to the right.

# NCS Solution



- User get a certificate from a CA
- The certificate and corresponding private key are saved on store device such as HDD or Usbtoken, or Smartcard
- The user uses the certificate to login on system
- The user manages certificate by certificate management anywhere

# Integrated component

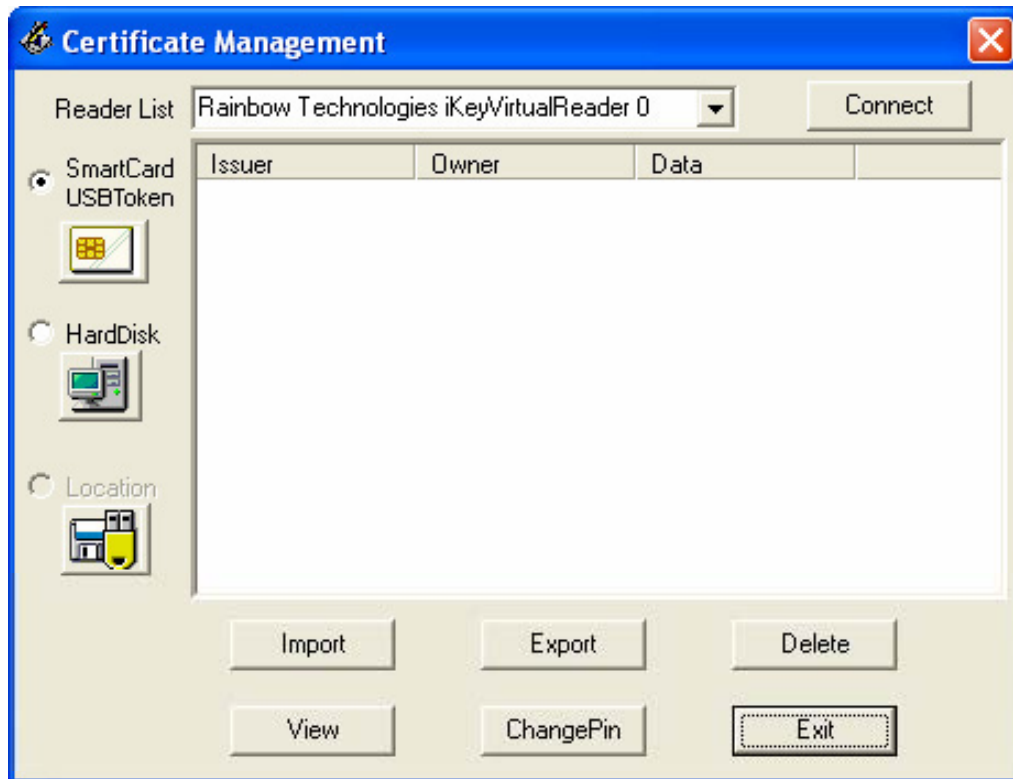
The screenshot shows an internet banking interface. On the left, there are navigation tabs for 'Personal' and 'Business' under 'Internet Banking', and an 'Exchange' table with three rows of CAD data. Below that is a 'Fee table' with a bar chart. The main area is titled 'LOGIN' with a key icon. There are two login options: 'Log-in with Certificate' (selected) and 'Log-in with User ID'. The 'Log-in with Certificate' option has a 'Log-in with Certificate' button circled in red. The 'Log-in with User ID' option has input fields for 'User ID' and 'Password' and a 'Log-in with User ID' button. A 'Certificate Management' dialog box is overlaid on the bottom right, showing a 'ProviderList' dropdown set to 'Gemplus GemSAFE Card CSP v1.0' and a table with columns 'Issuer', 'Owner', and 'Data'. The dialog also has 'SmartCard', 'HardDisk', and 'Location' radio buttons and 'View', 'OK', and 'Cancel' buttons.

CAD	999999	1999999
CAD	888888	1888888
CAD	777777	1777777

Issuer	Owner	Data
--------	-------	------

- DLL Package
- ActiveX controls
- Easy integrate to any existing system

# Certificate Management



- Easy integrate to web client
- No need to install smartcard driver
- Support many kind of smartcards

# Certificate Management



## Manage certificates on Smartcard & USB Tokens

- View Certificate List of Smartcard
- Import certificate from PFX file to Smartcard
- Change pin code of smartcard
- Delete certificate on Smartcard
- Export certificate from smartcard
- Check status and validate Certificate

# Certificate Management

Issued To	Issued By	Expiration Date
Katsuo.Chujo	GlobalSign PersonalSi...	10/23/2008
Kevin Blackman (WI...	WISeKey CertifyID A...	4/9/2009
Masakazu.Asano	GlobalSign PersonalSi...	4/21/2009
nguyen tuan anh	UTN-USERFirst-Client ...	6/11/2009
Thawte Freemail M...	Thawte Personal Free...	6/10/2009




## Manage certificates on System

- View Certificate List on System
- Delete certificate on system
- Export certificate from system
- Export certificate to PFX file
- Import certificate to system from PFX file
- Check status and validate Certificate



**DEMO**



# Q&A