

Egyptian E-Signature and Its role in Workflow Automation for Smart Ports



Dr. Sherif Hazem

VP Electronic Transactions Security, ITIDA



The Need For Authentication Systems and PKI Problem Definition ??

Bank Hackers Steal \$300 Millions via Malware

By DAVID E. SANGER and NICOLE PERLROTH
FEB. 14, 2015



“The goal was to mimic their activities,” said Sergey Golovanov of Kaspersky, about how the thieves targeted bank employees.

Credit Raphael Satter/Associated Press

Cyber Threats (Phishing) Allover The World

Crimeware and Phishing

Websense Global Threat Intelligence

Read about security research as it happens. Obtain in-depth security information including, research & statistics, white papers, presentations and the latest threat maps that display the most recent data collected by Websense Security Labs.



Select Date Range

Last 12 months

Select Attack Type

Phishing

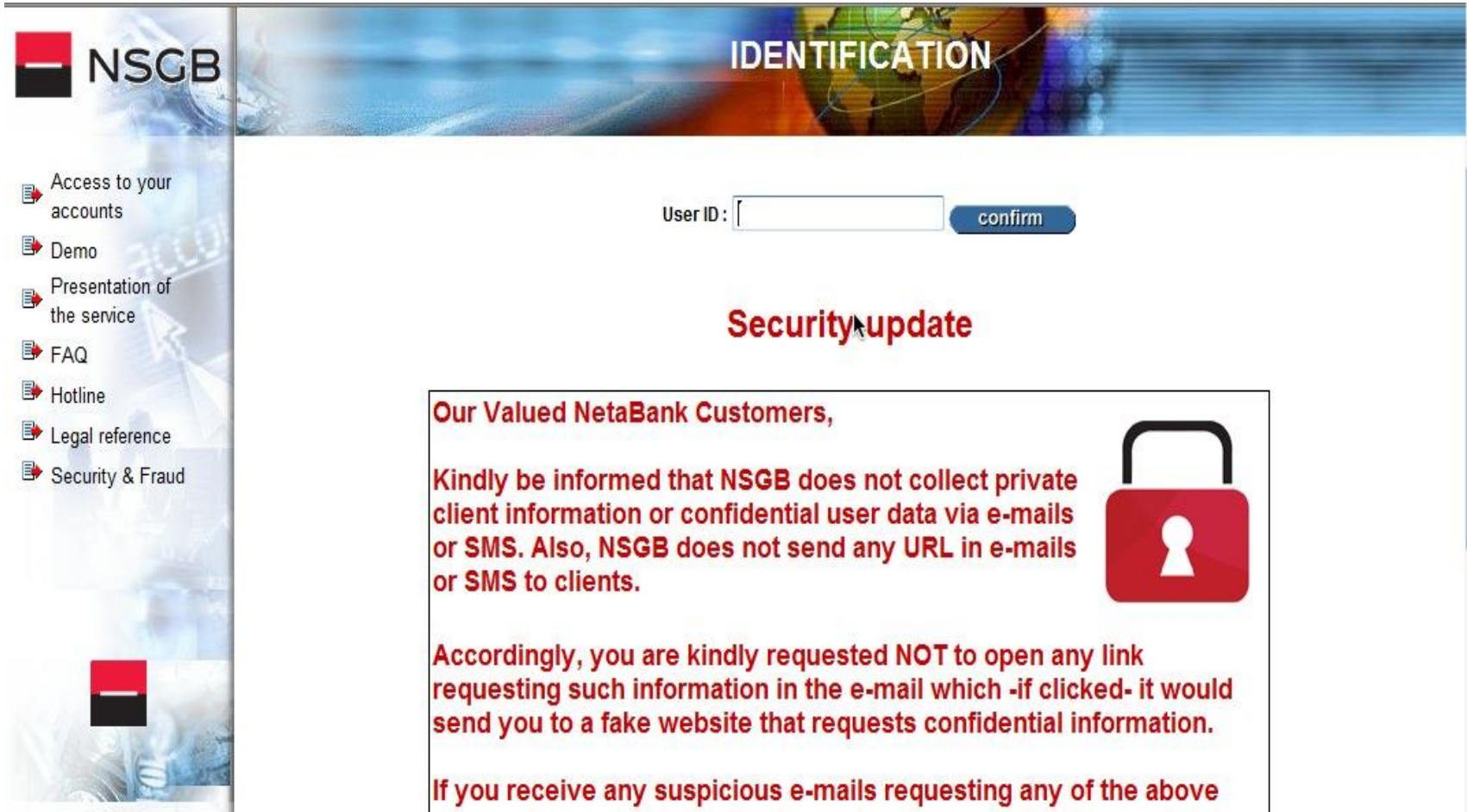
Update

Technical Solutions to The Problems at a Hand

Authentication Systems

- The most common forms of authentication systems can be :
 1. Shared Secrets (Passwords)

1. Shared Secrets - Passwords (One Factor Authentication) Examples



The screenshot displays the NSGB website interface. On the left is a navigation menu with the NSGB logo at the top and several menu items: 'Access to your accounts', 'Demo', 'Presentation of the service', 'FAQ', 'Hotline', 'Legal reference', and 'Security & Fraud'. The main content area features a header with the word 'IDENTIFICATION' and a login form with a 'User ID:' label, an input field, and a 'confirm' button. Below the login form is a red 'Security update' notification box. The notification text states that NSGB does not collect private client information or confidential user data via e-mails or SMS, and does not send any URL in e-mails or SMS to clients. It also requests users not to open any link requesting such information in an e-mail, as it would lead to a fake website. The notification includes a red padlock icon.

NSGB


IDENTIFICATION

User ID: [confirm](#)

Security update

Our Valued NetaBank Customers,

Kindly be informed that NSGB does not collect private client information or confidential user data via e-mails or SMS. Also, NSGB does not send any URL in e-mails or SMS to clients.




Accordingly, you are kindly requested NOT to open any link requesting such information in the e-mail which -if clicked- it would send you to a fake website that requests confidential information.

If you receive any suspicious e-mails requesting any of the above

1.Shared Secrets -Passwords (One Factor Authentication) Examples Cont..

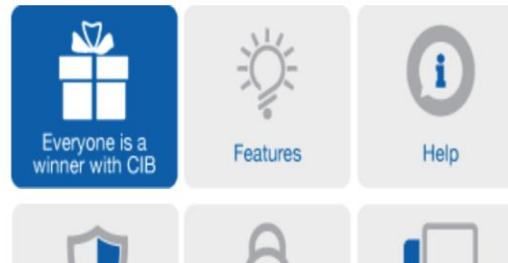


Register, transact on
CIB Internet Banking
and win a Tablet

 Username

Password

Sign In



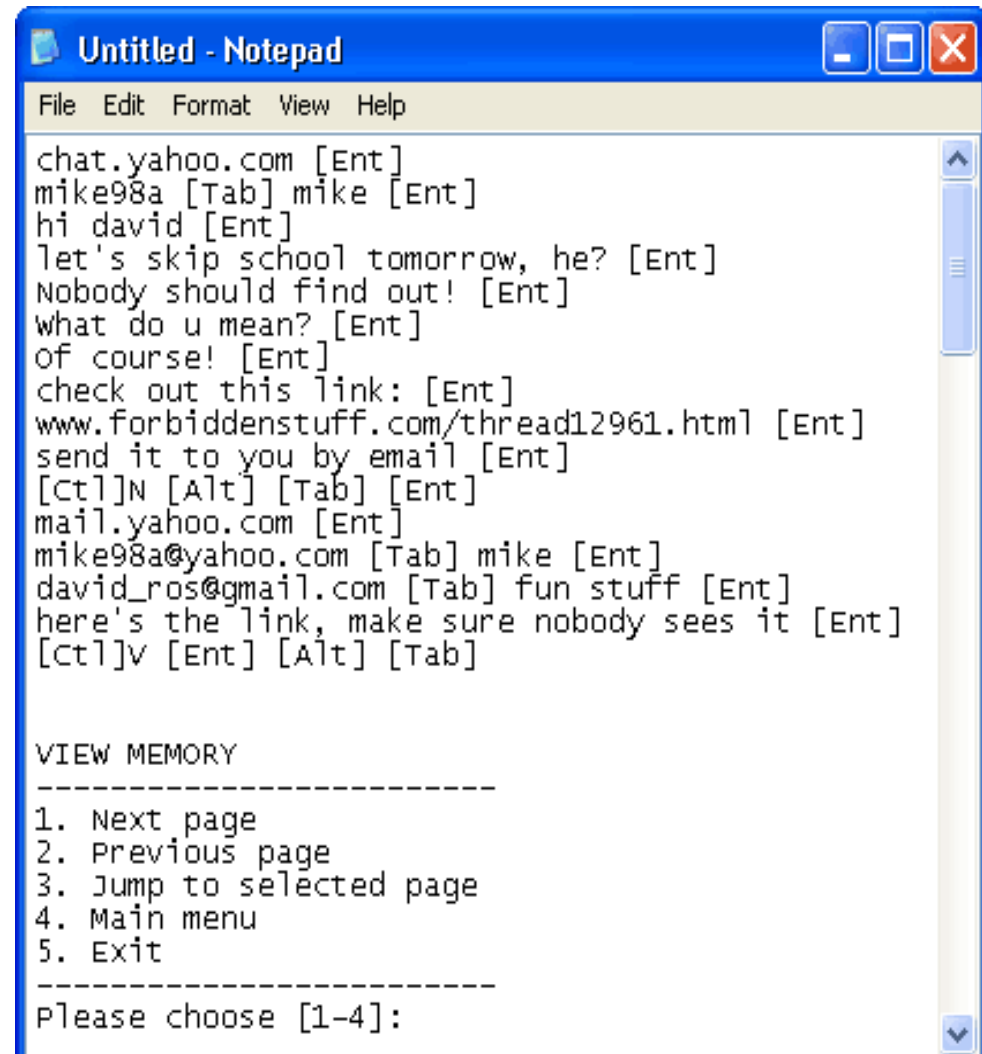
Attacks on Password Techniques : Password Cracking

Figure 2: A Password Cracking Program



Source: *Zip Password*

Attacks on Password Techniques :Keystroke Logger



Authentication Systems

- The most common forms of authentication systems can be classified into three main classes:
 1. Passwords
 2. Time Based Password (One Time Password)
 3. Biometrics

2. Time-Based -One Time Password (Two Factor Authentication)



time-based one-time password

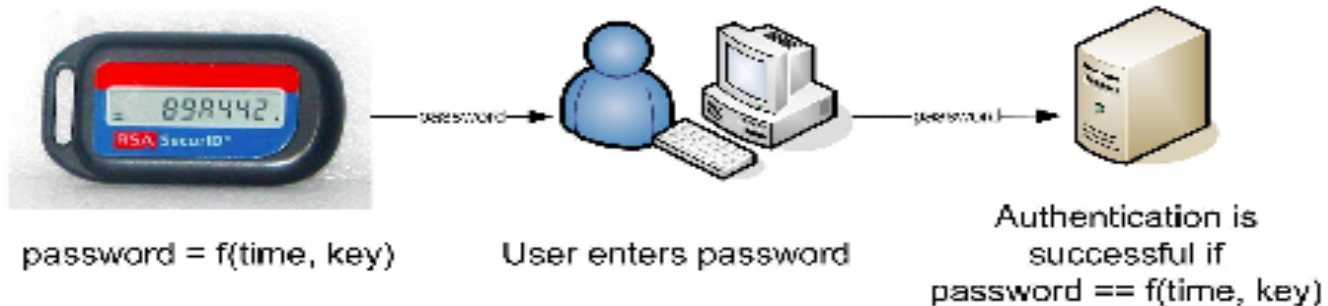


Illustration 5: One Time Password based on time

Samples of Phishing Attack on OTP

Citibank Phish Spoofs 2-Factor Authentication



[privacy](#) [citibusiness.com](#)

E-mail Security Zone
Valued Customer ATM/Debit card ending in: verify

CitiBusiness E-mail & Security Banking Alerts

We are committed to protecting you, with the latest technology to keep your details secure, and dedicated teams to monitor online activity and intercept any suspicious actions. And we do everything we can to protect our online customers, but the steps we take can be much more effective if you work with us to protect yourself.

06/27/2006 our security system detected an unsuccessful access attempt to your online account from IP address **81.190.253.29** that does not correspond to your current address.

Please [click here](#) to confirm your current address or change it online.

If you do not confirm your address until 06/30/2006 your account will be SUSPENDED for security reasons and we will send you an Activation Code by post which you will need to renew your online banking service access. You will receive this within seven days if your current address is not confirmed.

E-mail Security Zone

At the top of this message, you'll see an E-mail Security Zone. Its purpose is to help you verify that the e-mail was indeed sent by Citibank. If you have questions, please call 1-800-374-9700. To learn more about fraud visit Citibank.com and click "about e-mail fraud" at the bottom of the screen.

Continue...



CitiBusiness® Online

For enrolled CitiBusiness Online users only!

Enter Business Code and click Enter.

Business Name: Guest

Enter Business Code: 7000-0000-

0	1	2	3	4	5	6	7	8	9
Back			Clear			Enter			

The business code contains 16 digits and begins with '70000000'

For Personal Banking, sign on to [Citibank Online](#)

Continue...



CitiBusiness® Online

I am unable to sign you on to CitiBusiness® Online at this time.

7000000008453550 is not a recognized Business Code.
Please close this window and try signing on again.

You can contact customer service at 1 (800) 285 1709.

For hearing impaired call 1 (800) 788 0002

[Click here to QUIT and Close this Window](#)

Continue..

Bank of America Higher Standards


Online Banking


Online Banking Alert

Your Online Banking is Blocked

Need additional up to the minute account information?
Sign In »

Because of unusual number of invalid login attempts on you account, we had to believe that, their might be some security problem on you account. So we have decided to put an extra verification process to ensure your identity and your account security. Please click on [sign in to Online Banking](#) to continue to the verification process and ensure your account security. It is all about your security. Thank you, and visit the customer service section.

Bank of America, N.A. Member FDIC. [Equal Housing Lender](#) 
© 2007 Bank of America Corporation. All rights reserved.

Official Sponsor 2000-2004 U.S. Olympic Team 

http://goodbox-pc.com/www.bankofamerica.com/BOA/sslencrypt218bit/online_banking/index.htm

Authentication Systems

- The most common forms of authentication systems can be classified into three main classes:
 1. Passwords
 2. Smart Cards
 3. Digital Certificate and PKI (E-Signature)

E-Signature and PKI Systems & Human Digital Identity

Electronic Signature

Electronic Signature means an electronic symbol, attached to a document and executed or adopted by a person with the intent to sign the document

- Source: Electronic Signatures in Global and National Commerce Act (E-Sign)

What is Meant by An Electronic Signature ?



Continue....

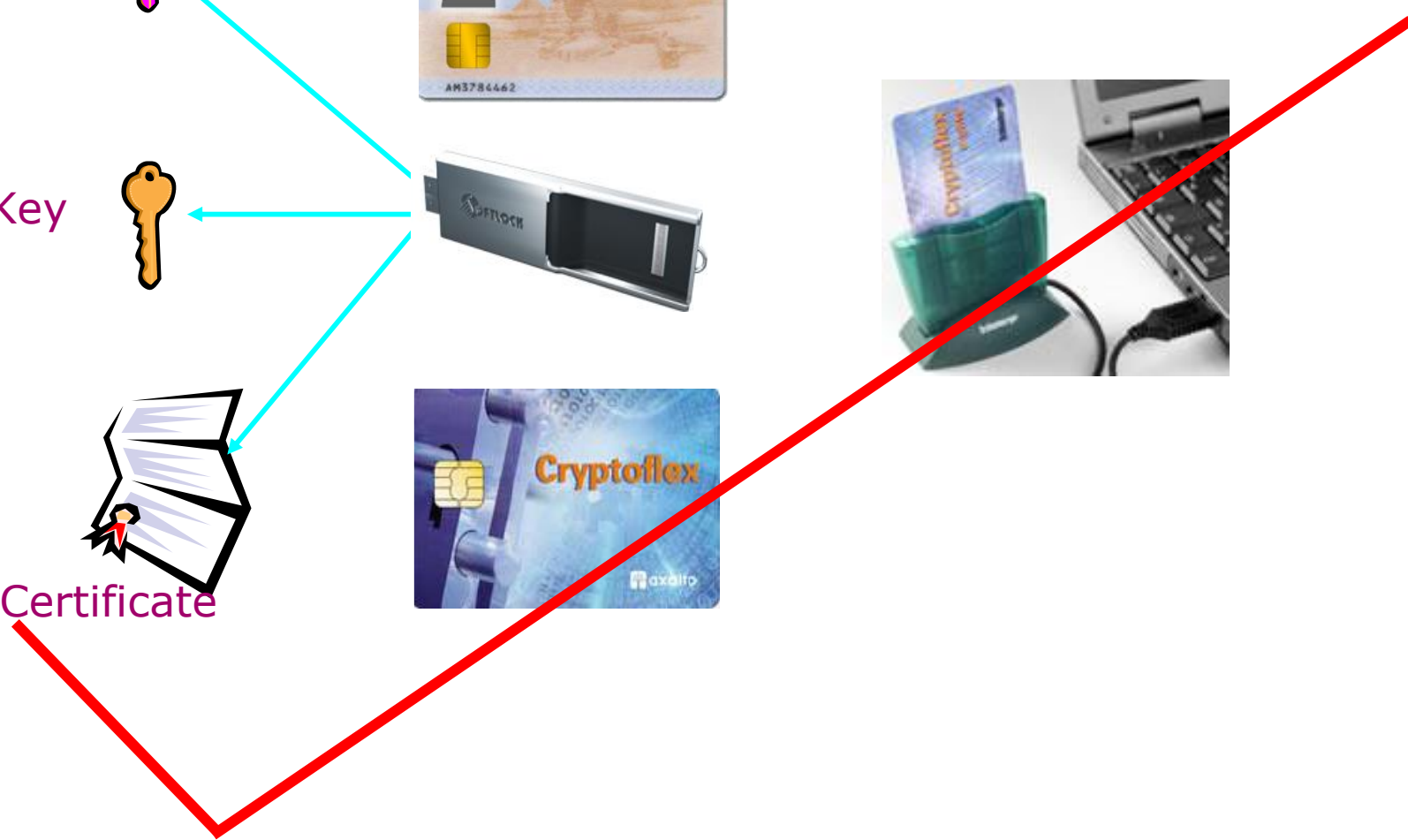
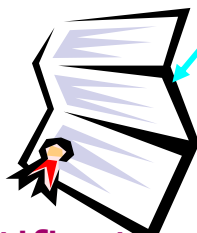
Private Key



Public Key



Digital Certificate



Egyptian Government Efforts

- In April 2004, Egypt passed the Law 15 Regulating Electronic Signatures (or the “E-Signature Law”)
- The E-signature Law also established the E-signature regulatory authority, officially known as the **Information Technology Industry Development Agency (ITIDA)**.
- The E-Signature Law supports E-commerce in Egypt by enabling Egyptians to use the Internet and to enter into contracts securely by making the Internet a legally viable medium for online sales, without the need to sign the document physically.

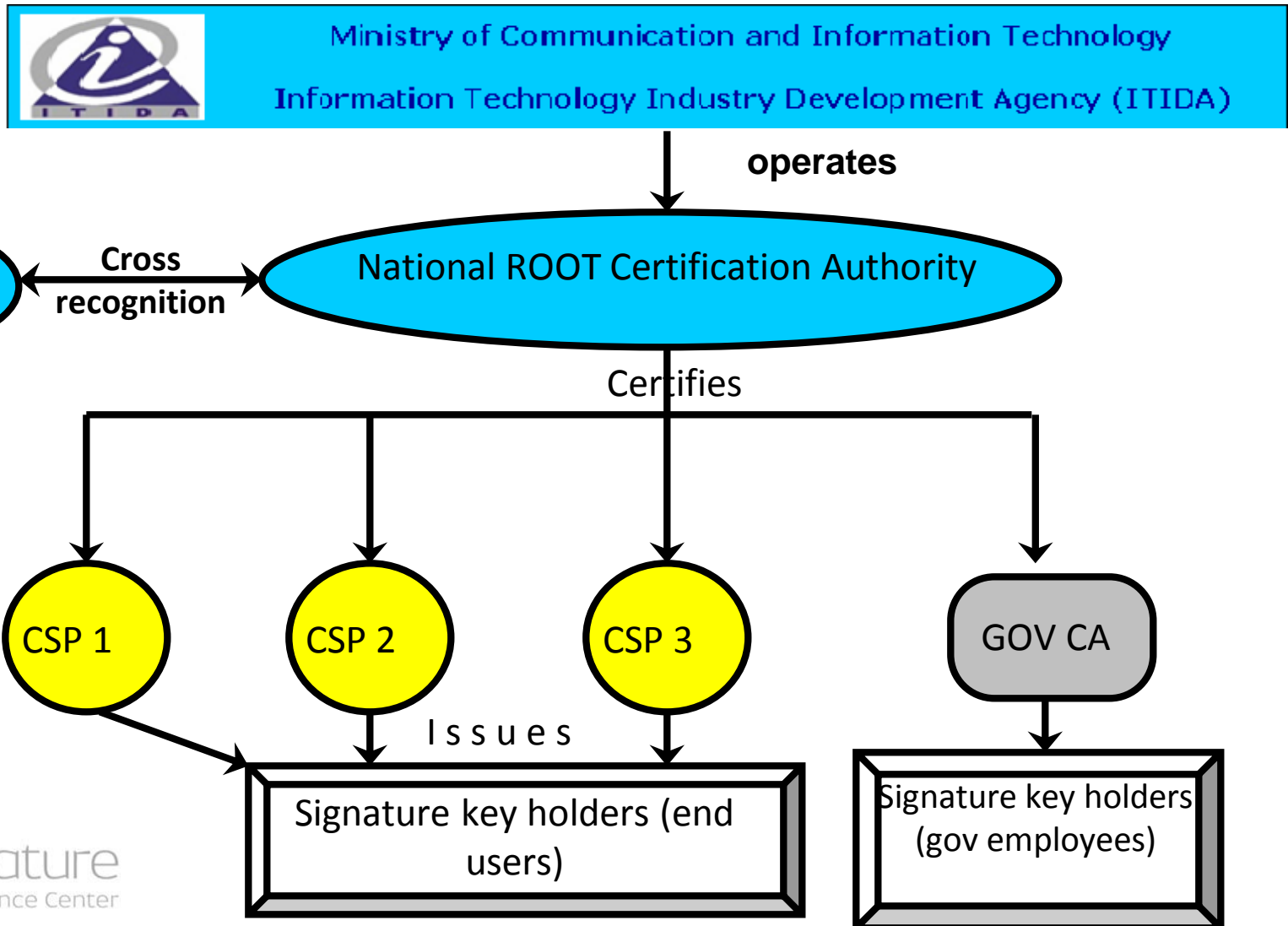
E-Signature Infrastructure Establishment Time-Based Progress

- **April 2004** : The president issued the e-signature Law
- **May 2005**: The E-signature Executive Directives was published
- **May 2005-February 2006**: Inviting companies to apply for e-signature license and approving 4 Licenses.
- **May 2006**: Publishing the Root CA RFP.
- **February 2007**: Start working with G&D vendor in preparing the site and installing hardware and software.
- **September 2009**: Inauguration of the Root CA main site with attendance of the prime minister and minister of communication and advanced technology

E-Signature Infrastructure Establishment Time-Based Progress

- **January 2010:** SNS obtained a work permit and get connected to Egyptian Root CA main site.
- **August 2010:** Egypt Trust and MCDR obtained E-signature work permits form ITIDA and connected to Egyptian Root CA main site.
- **May 2012:** Starting the deployment phase of E-signature applications with 12 pilot projects in different sectors in the government , Banking, and financial sectors
- **June 2012:** Governmental CA accomplished their infrastructure and obtained E-signature work permits form ITIDA and connected to Egyptian Root CA main site.
- **August 2013:** Inaugurating the E-signature Competence Center

ITIDA Roles in E-Signature



ROOT CA Main Site Achievements

Achievements.....



- Root CA main trust center with 6 IT fortified rooms and more than 40 different types of servers and security equipments has been implemented to operate 24/7 **by 100% highly trained Egyptian staff.**
- Three private CSPs are ISO 27001 certified and passed ITIDA audit (financial, legal and technical).
- The Three deployed private CSPs have been securely connected to the Root CA main trust center to maintain a copy of all the issued digital certificates and CRLs to maintain client rights in case of disaster and are ready to issue digital certificate private sector under the hood of Egyptian Root CA.

Pictures from Reality..& Practical Success Stories

E-Signature Products

- Home made E-signature tools are ready to be used
 - **(Egyptian Smart Token (with and without Fingerprint)).**
 - **Infrastructure Software Components have been implemented inside ITIDA E-Signature Lab to work with different types of Operating systems (MS-Windows, Linux, Unix Solaris 10 OS).**
 - **E-Signature Applications (Desktop, Web, and Mobile).**

E-Signature Tools



**Egyptian
National IDs**



BIOMETRIC

PROFESSIONAL

STANDARD

Egyptian Smart Tokens



**National IDs
Readers**



Crypto-Micro-SD

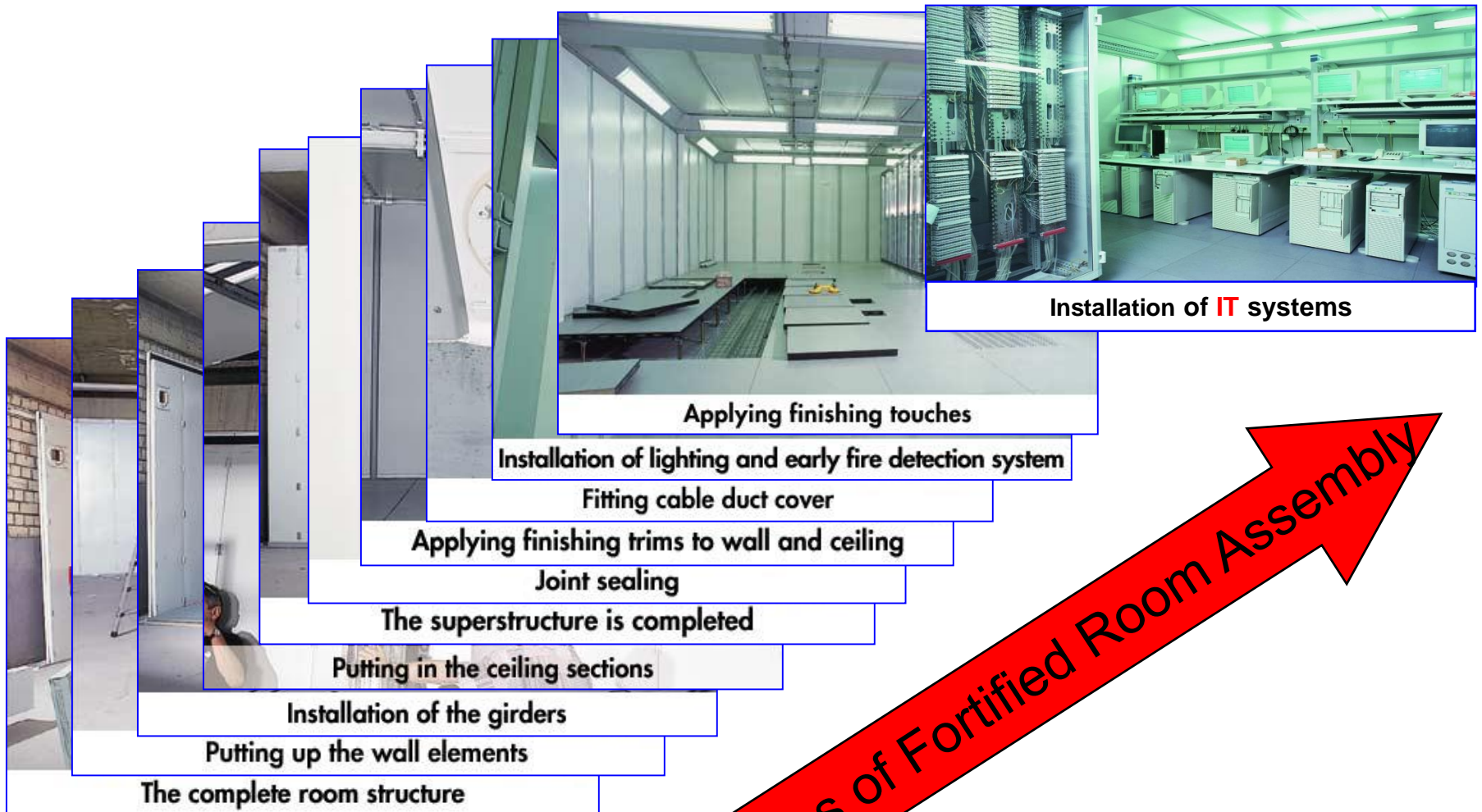


Crypto-Sim Card

Fortified Room Door Sample



IT Room assembly - step by step



Steps of Fortified Room Assembly

00 :00 :00 :00



Practical Success Stories

الرئيسية
خروج

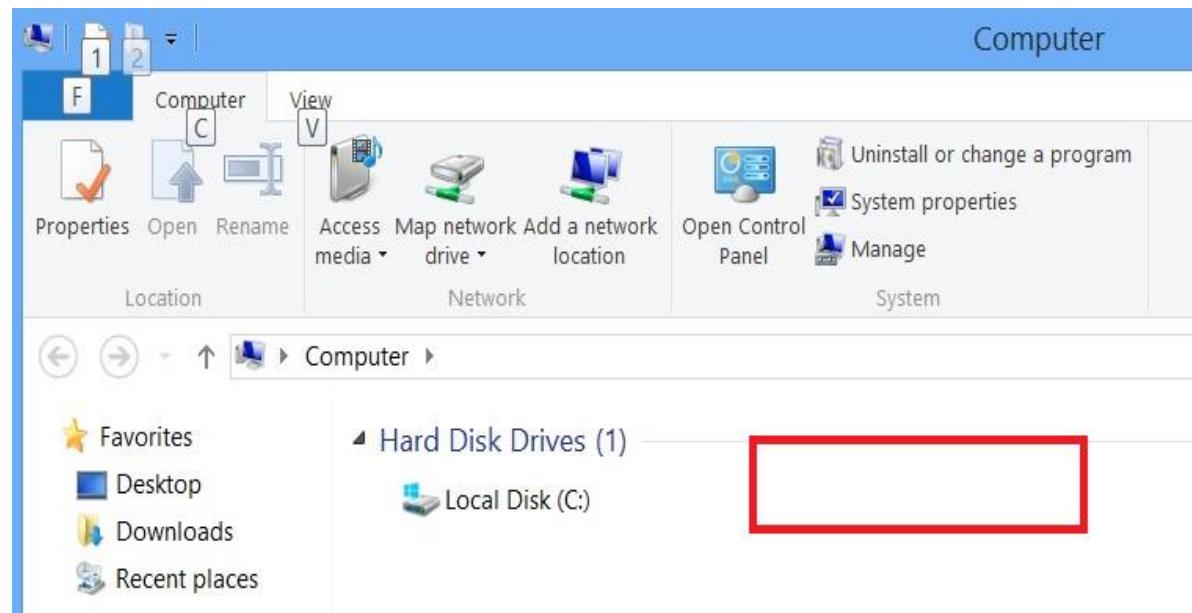
نظام إدارة الاجتماعات



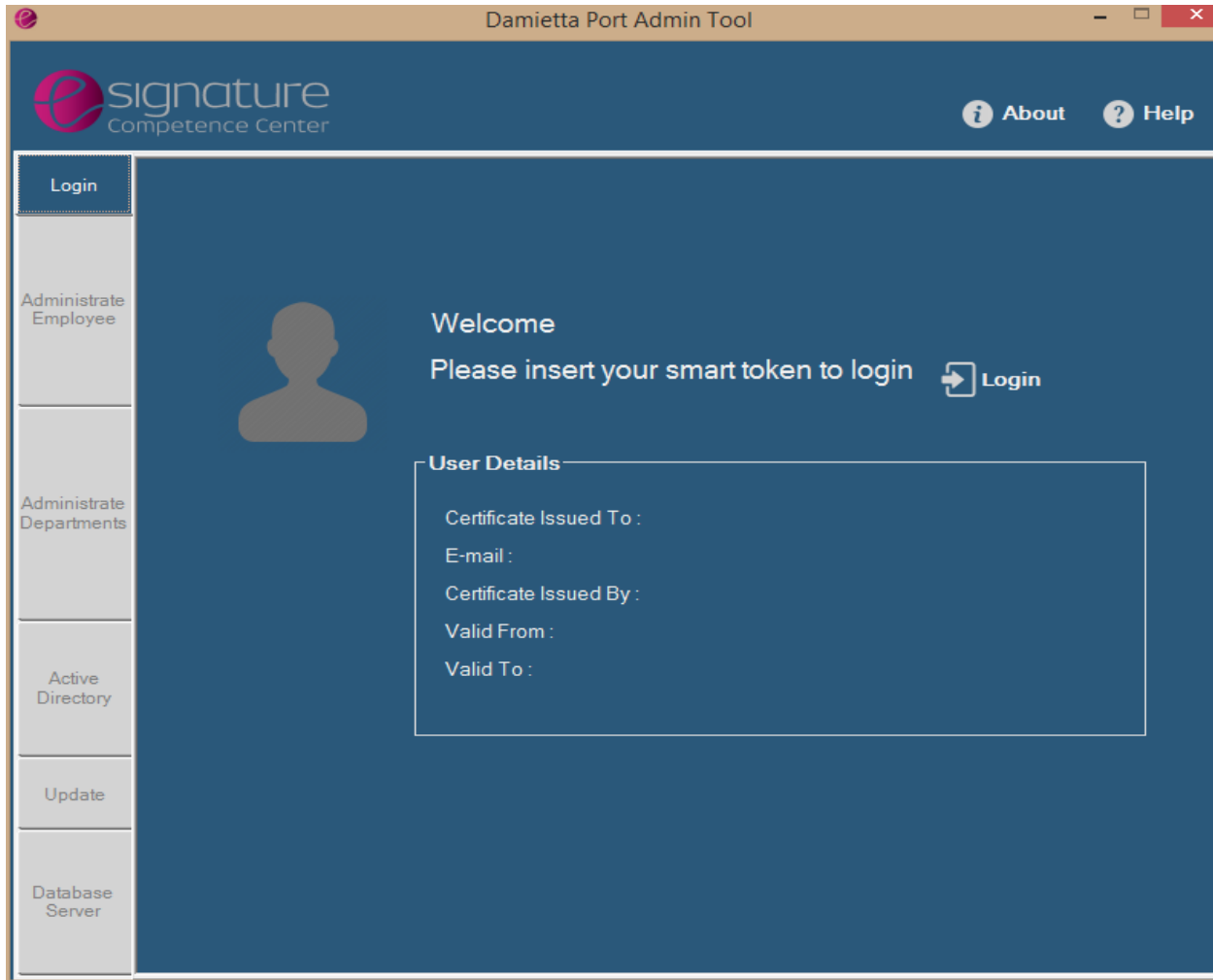
قرارات الاجتماع	م حضر الاجتماع	عرض اجندة الاجتماع	عنوان الاجتماع	تاريخ الاجتماع
			اجتماع مجلس الإدارة	23/01/2013
			اجتماع مجلس الوزراء	18/01/2013

- الرئيسية
- الاجتماعات
- م حضر وقرارات الاجتماع
- بحث عن الاجتماعات
- بيانات المستخدمين
- دليل المستخدم

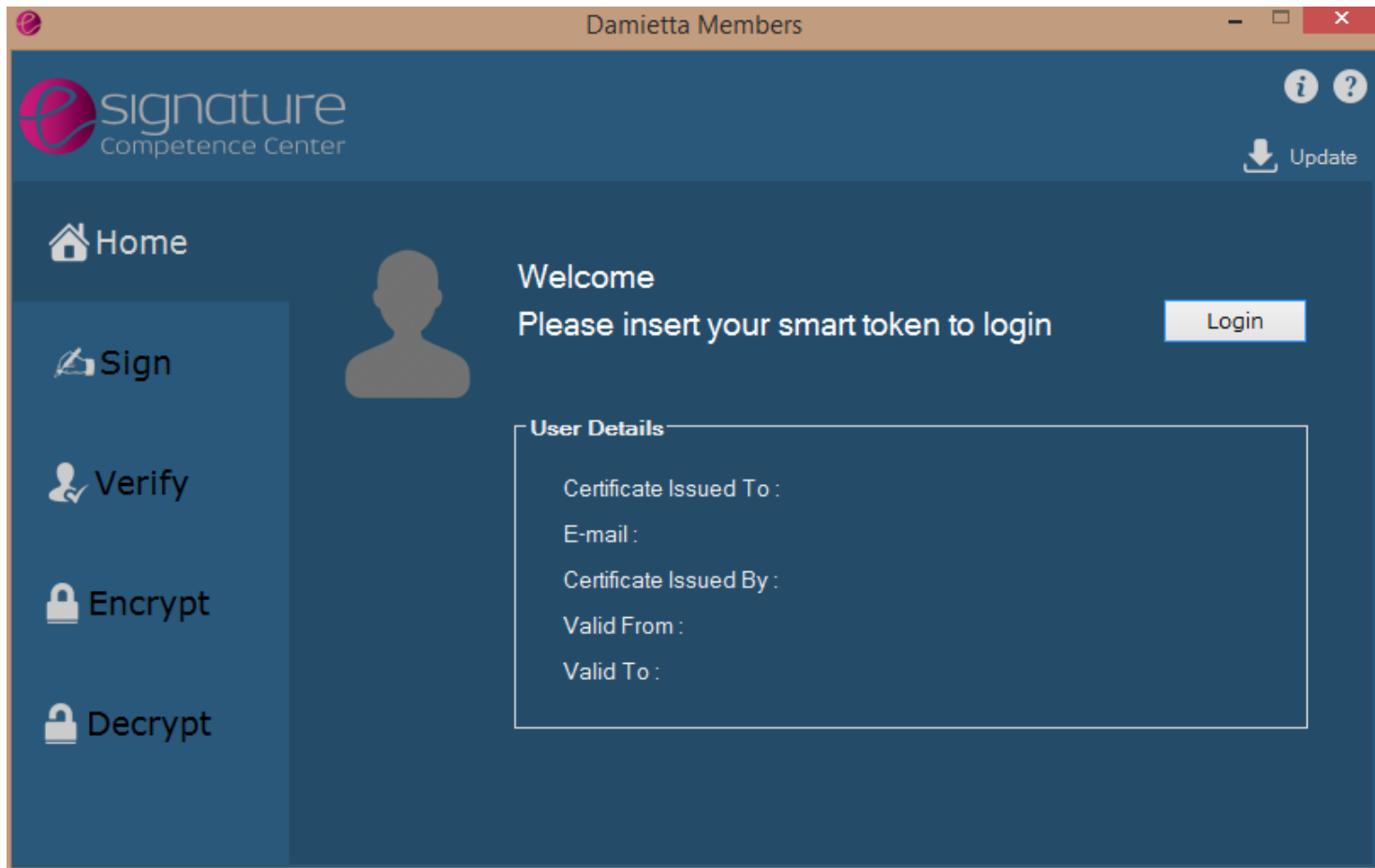
Success Stories Samples Cont....



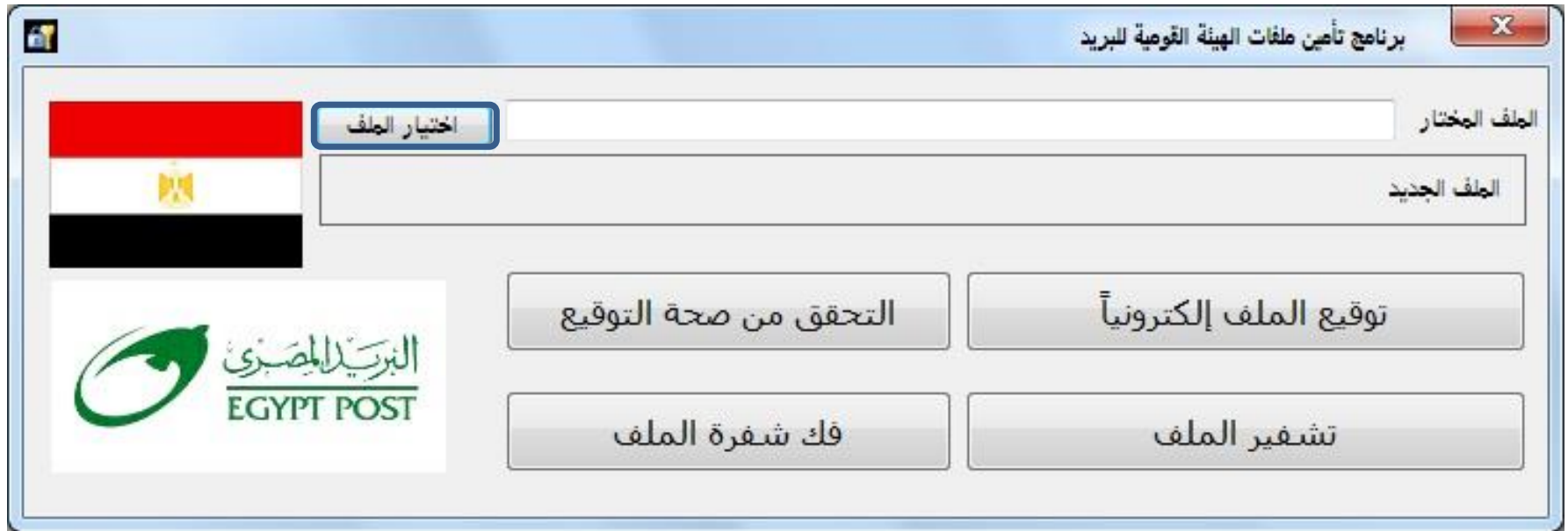
Damietta Port Documents Management Work Flow



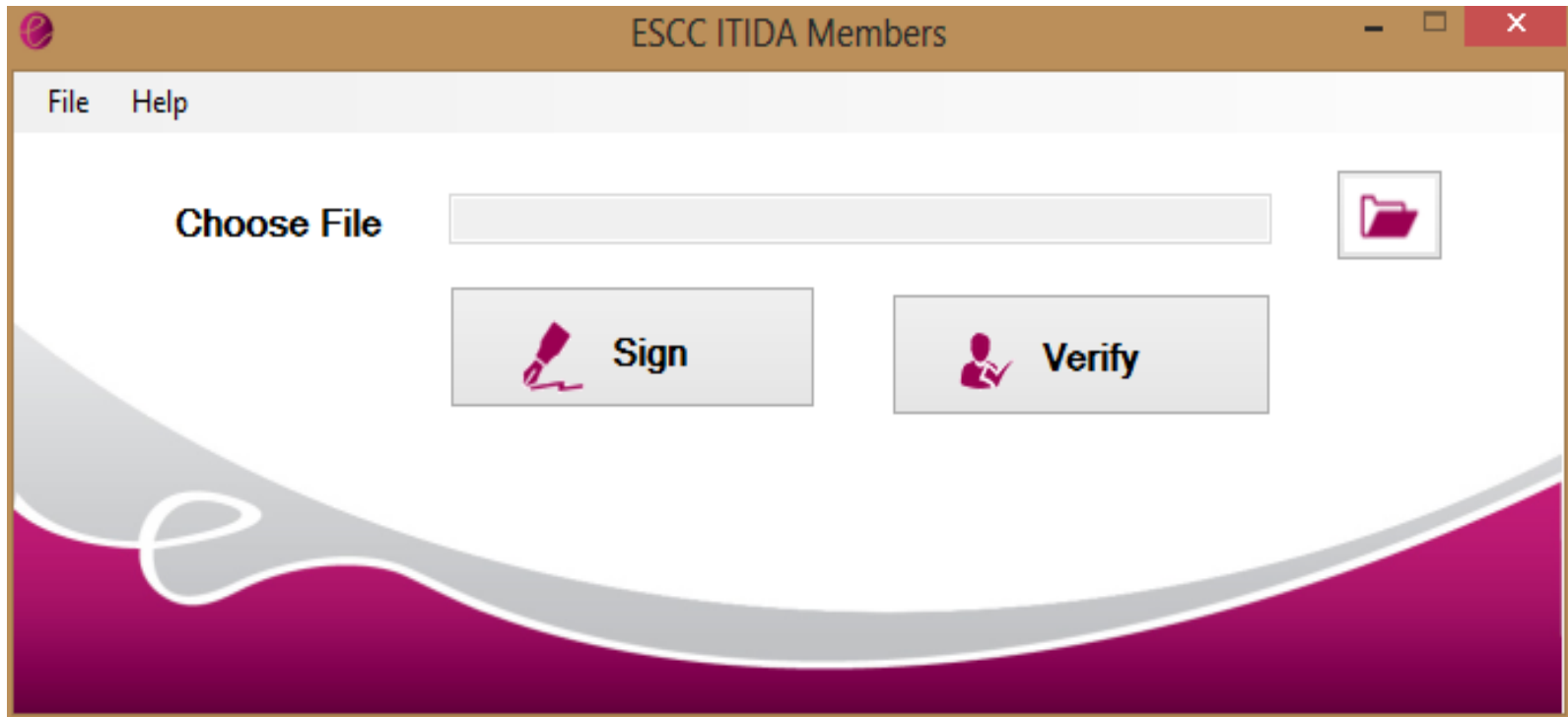
Damietta Port Documents Management Work Flow



Egypt Post Documents Management Work Flow

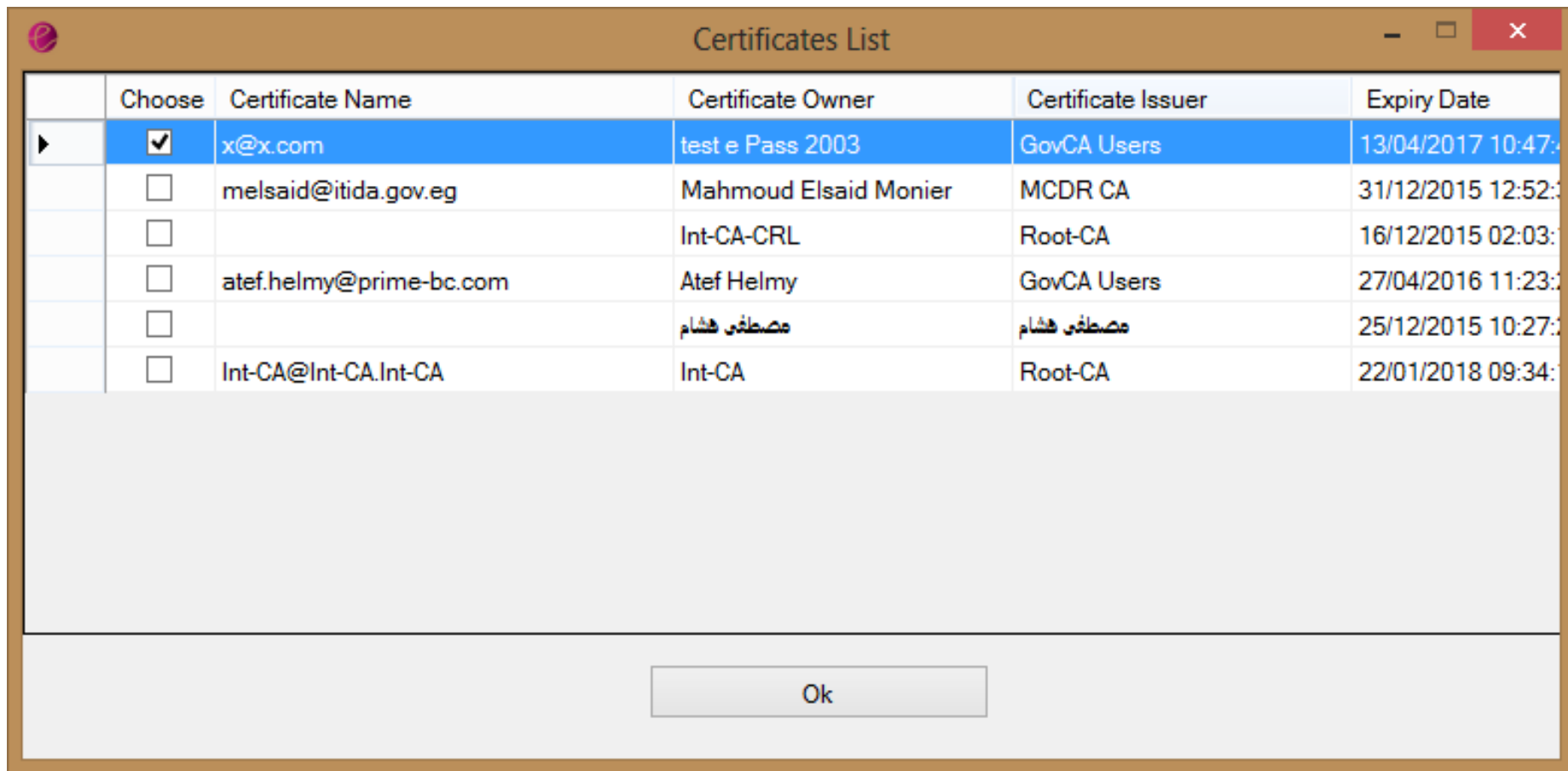


ITIDA members document work flow s/w

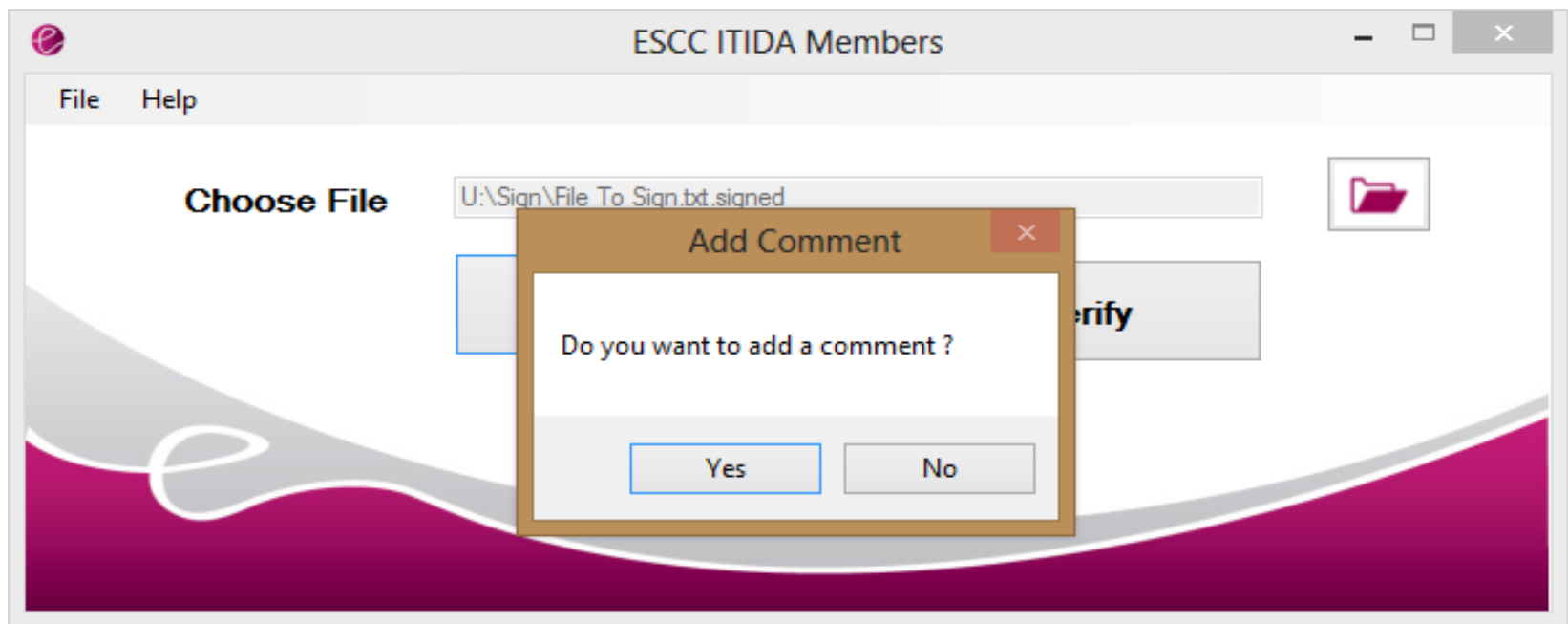


ITIDA members document work flow s/w...

Choose certificate to sign with

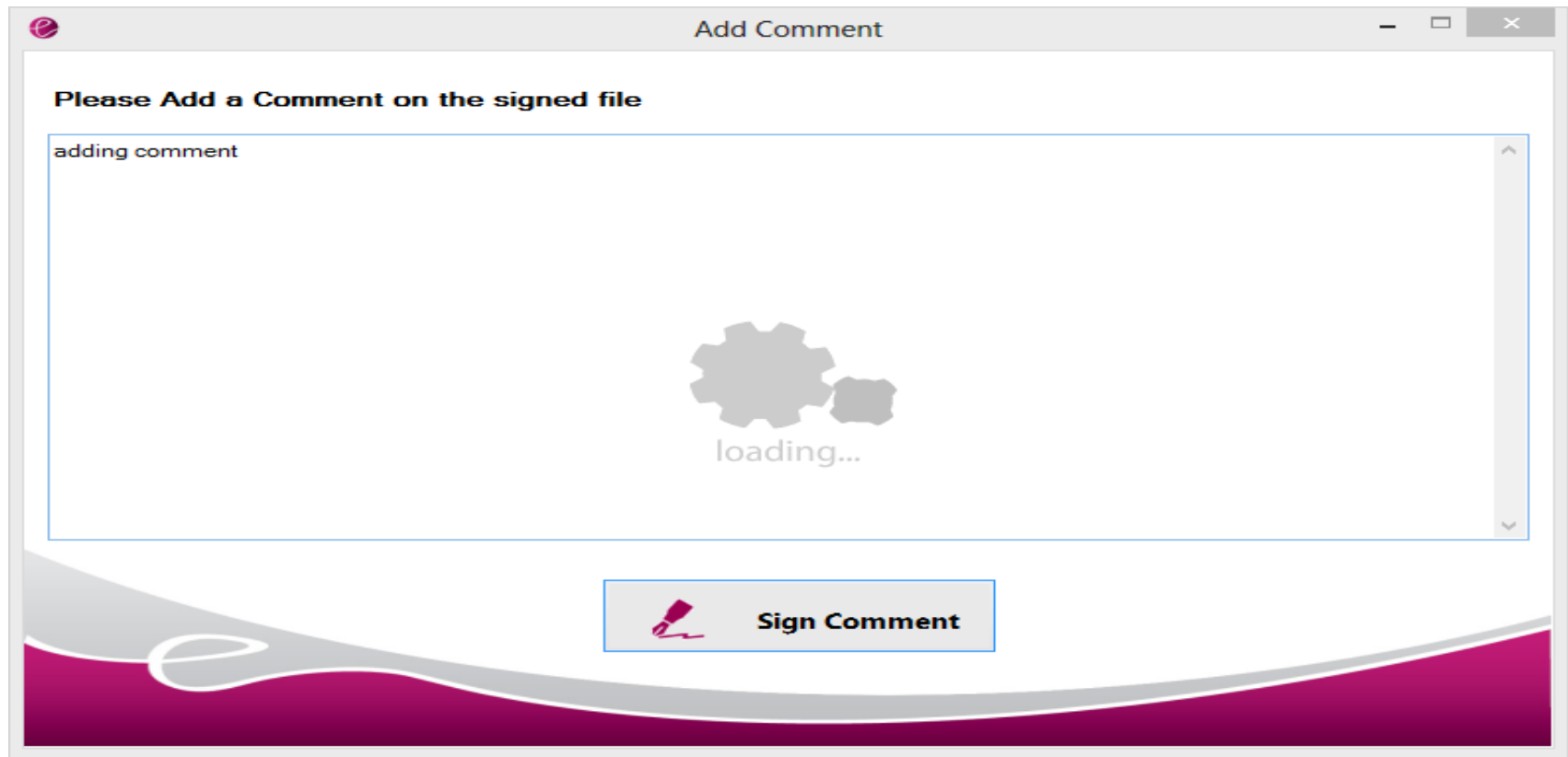


ITIDA members document work flow s/w... Adding a comment



ITIDA members document work flow s/w...

Signing the added comment



ITIDA members document work flow s/w...

View signed comments (1)



ITIDA members document work flow s/w... Viewing comments (2)



بيانات القرائير		رقم	الحتم ذو التاريخ		
رقم	التاريخ			جنيته	قرش
مصلحة					
قسم					
المبلغ المستحق إلى					
بموجب } الطلبات طيه ، أو :					
صار مراجعته ووجد على صحة ومقدم لاعتماده إداريا وصرف القيمة بواسطة					
إذن صرف على					
شيك على البنك المركزي في					
شيك على الخارج } صاحب الحق أو :					
يسحب باسم					
ويرسل إليه بالعنوان الآتي :					
الجملة					

رقم _____

الحتم ذو التاريخ _____

كتب المراجعة _____

رئيس القسم _____

٢

تقيد في السجل برقم _____		الكاتب المنوط _____	
عدد المرفقات	الاعتماد الإداري ونوع الخصم		الحتم ذو التاريخ
	بيانات	نوع الخصم	
		قرش	جنيته
		قسم	جنيته
		فرع	جنيته
		فصل	جنيته
		بند	جنيته
		إجمالي الأصل	جنيته
		قرش	جنيته
		بيانات الاستقطاعات	جنيته
		عادي	جنيته
		إضافي	جنيته
		دمغة توقيع	جنيته
		قرش	جنيته
		رسم الدمغة	جنيته
		صافي القيمة المطلوب صرفها	جنيته
		علامة	جنيته
		في _____ سنة ٢٠٠	جنيته
		الإمضاء _____	جنيته
		الإمضاء _____	جنيته
		الإمضاء _____	جنيته

رئيس المصلحة _____

١١) إقرار كاتب سجل الحجوزات والتنازلات : _____

١٢) إقرار بأن القيمة مرتبط بها على الاعتماد المخصص وأن البند المختص يسمح ولم يسمح الصرف : _____

(أو) بأن المبلغ مضاف بحساب : _____

الإيرادات _____

بتاريخ _____

الهيئة العامة لشئون المطابع الأميرية ٢٠٠٦ - ٢٠٠٧

تقيد في سجل رقم ٥٥ ج ح ع برقم _____		الكاتب المنوط بالسجل _____	
عدد المرفقات	الاعتماد الإداري ونوع الخصم		الحتم ذو التاريخ
	بيانات	نوع الخصم	
		قرش	جنيته
		قسم	جنيته
		فرع	جنيته
		فصل	جنيته
		بند	جنيته
		إجمالي الأصل	جنيته
		قرش	جنيته
		بيانات الاستقطاعات	جنيته
		عادي	جنيته
		إضافي	جنيته
		دمغة توقيع	جنيته
		قرش	جنيته
		رسم الدمغة	جنيته
		صافي القيمة المطلوب صرفها	جنيته
		علامة	جنيته
		في _____ سنة ٢٠٠	جنيته
		الإمضاء _____	جنيته
		الإمضاء _____	جنيته
		الإمضاء _____	جنيته

رئيس المصلحة _____

١١) إقرار كاتب سجل الحجوزات والتنازلات : _____

١٢) إقرار بأن القيمة مرتبط بها على الاعتماد المخصص وأن البند المختص يسمح ولم يسمح الصرف : _____

(أو) بأن المبلغ مضاف بحساب : _____

الإيرادات _____

بتاريخ _____

الهيئة العامة لشئون المطابع الأميرية ٢٠٠٦ - ٢٠٠٧

تقيد في سجل رقم ٥٥ ج ح ع برقم _____		الكاتب المنوط بالسجل _____	
عدد المرفقات	الاعتماد الإداري ونوع الخصم		الحتم ذو التاريخ
	بيانات	نوع الخصم	
		قرش	جنيته
		قسم	جنيته
		فرع	جنيته
		فصل	جنيته
		بند	جنيته
		إجمالي الأصل	جنيته
		قرش	جنيته
		بيانات الاستقطاعات	جنيته
		عادي	جنيته
		إضافي	جنيته
		دمغة توقيع	جنيته
		قرش	جنيته
		رسم الدمغة	جنيته
		صافي القيمة المطلوب صرفها	جنيته
		علامة	جنيته
		في _____ سنة ٢٠٠	جنيته
		الإمضاء _____	جنيته
		الإمضاء _____	جنيته
		الإمضاء _____	جنيته

رئيس المصلحة _____

١١) إقرار كاتب سجل الحجوزات والتنازلات : _____

١٢) إقرار بأن القيمة مرتبط بها على الاعتماد المخصص وأن البند المختص يسمح ولم يسمح الصرف : _____

(أو) بأن المبلغ مضاف بحساب : _____

الإيرادات _____

بتاريخ _____

الهيئة العامة لشئون المطابع الأميرية ٢٠٠٦ - ٢٠٠٧

3



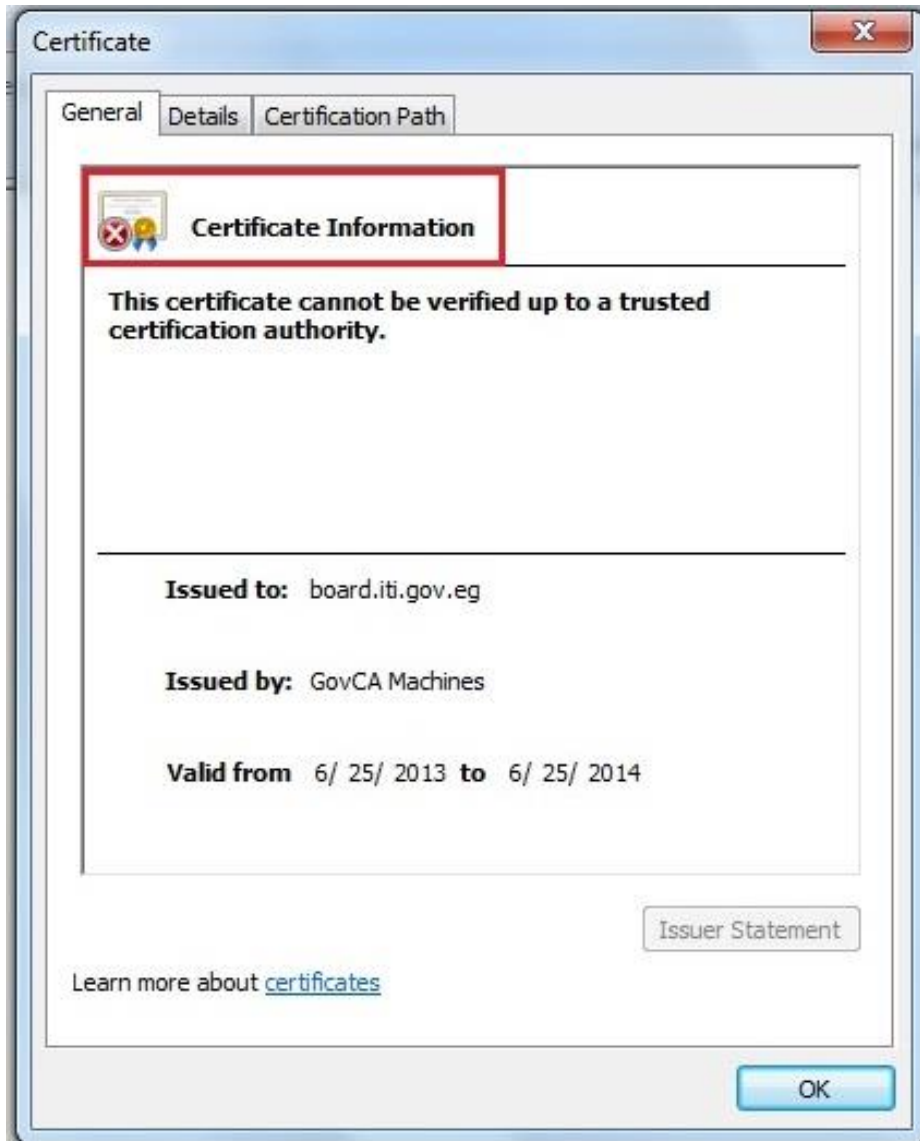
Digital Signatures Desktop Management



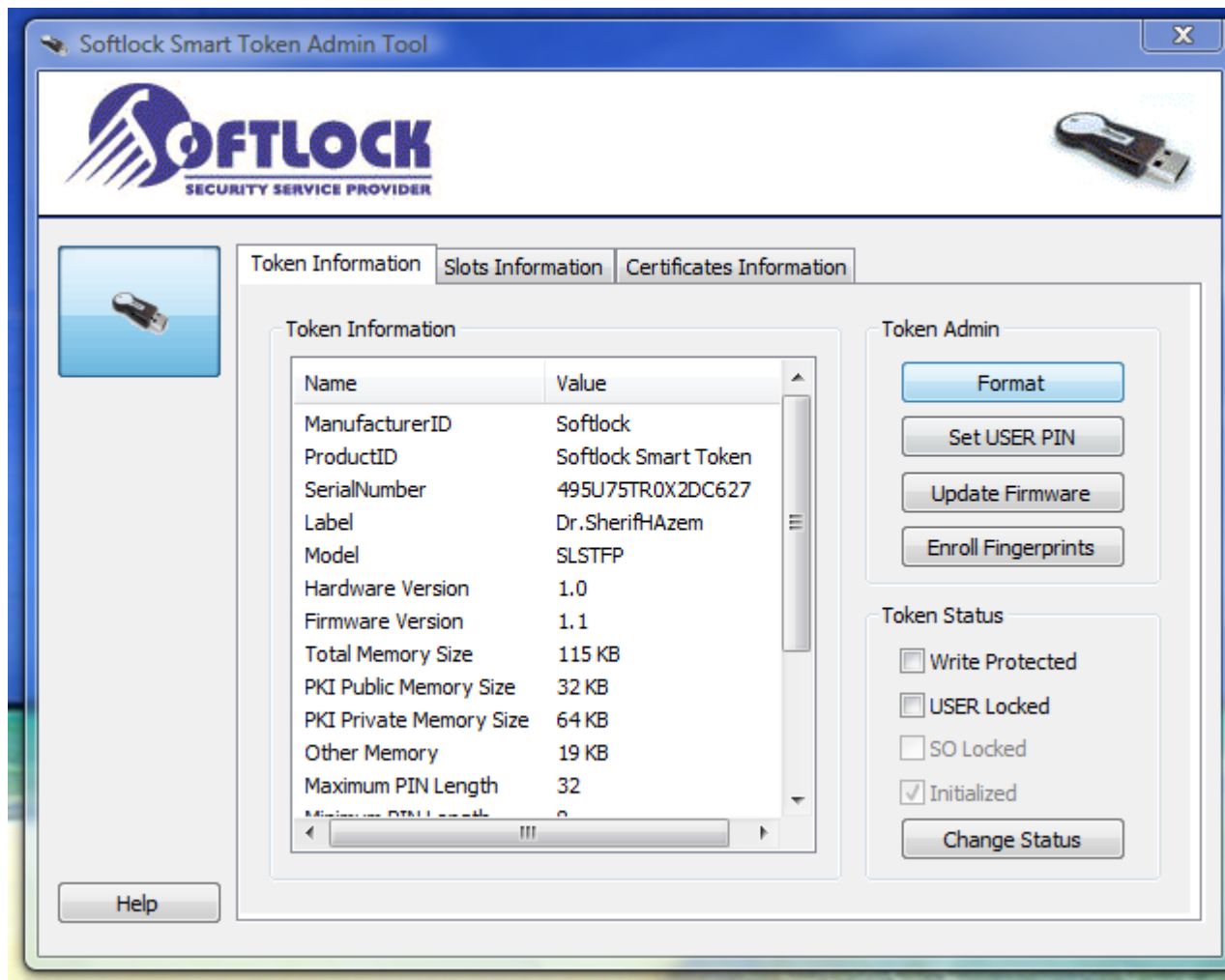
SSL Trusted Websites

The image shows a web browser window with the address bar displaying `https://board.iti.gov.eg/token_login.as`. A 'Website Identification' dialog box is open, indicating that 'EgyptRootCA has identified this site as: board.iti.gov.eg' and that 'This connection to the server is encrypted.' It asks 'Should I trust this site?' and provides a 'View certificates' button. A yellow padlock icon is highlighted with a green circle. To the right, a 'Certificate' dialog box is open, showing the 'Certification Path' with the following hierarchy: EgyptRootCA, GOVCA, GovCA Machines, and board.iti.gov.eg. The 'Certificate status' is 'This certificate is OK.' and there is an 'OK' button at the bottom.

Detection of Faked Sites



Smart Token Software



Mobile Stock Application Demo



Questions

????

Thank you