

**EFS - KMS**  
**Web based Key Generation Software**  
**(General User)**  
**(WKGSG) v1.0 User Manual**

---

---

**Singapore Network Services Pte Ltd**

**Release 1.0 – 14 January, 2002**

**Document Control Number \_\_\_\_\_**

## Table of Contents

<b>1</b>	<b>INTRODUCTION</b> .....	<b>1</b>
1.1	ABOUT THIS USER MANUAL.....	1
1.2	WKGSG APPLICATION.....	1
<b>2</b>	<b>WKGSG PROCEDURES</b> .....	<b>2</b>
2.1	KEY GENERATION SESSION.....	2
2.2	UPDATE SMART CARD.....	7
2.3	RESUBMIT PUBLIC KEY.....	9

# 1 Introduction

You must obtain a smart card from the CA Administrator before proceeding to generate your key pair using Web based Key Generation Software for General Users (WKGSG). You must also have the system generated smart card password to log into WKGSG. We also assume that WKGSG plug-ins has been successfully installed on your computer.

---

## 1.1 About This User Manual

This user manual takes you through the process of generating your own key pair and updating your smart card with the certified public key using WKGSG.

The WKGSG functionality is presented in the form of step by step procedures. The first set explains how you can generate your public and private key pair, and the second set explains how you can update your smart card.

The last section describes how to resubmit your public key in case the smart card update process fails.

---

## 1.2 WKGSG Application

WKGSG verifies the state of the process (key generation or update smart card) when you log in and accordingly guide you through the subsequent steps.

## 2 WKGSG Procedures

After submitting your certificate application to the CA, you will be issued a smart card, together with a sealed mailer containing the system generated password of your smart card. You will use this smart card and password, to access the WKGSG application, and generate your own public and private key pair.

### 2.1 Key Generation Session

Before you initiate the KGSG session, make sure that

- You have your personal smart card and sealed mailer.
- The smart card reader is connected properly to the port configured during installation.

#### To generate the public key – private key pair

1. Insert your smart card into the smart card reader.

**Note:** You must not remove the smart card from the smart card reader after the login procedure, until the end of the key generation session.

2. Login to the EFS application using your UserID/Password. Click on the KGSG link on the main menu in the EFS page. The **WKGSG - Licence Agreement** screen (Figure 1) will be displayed. You are allowed to login only after you have agreed to the terms and conditions in the agreement.

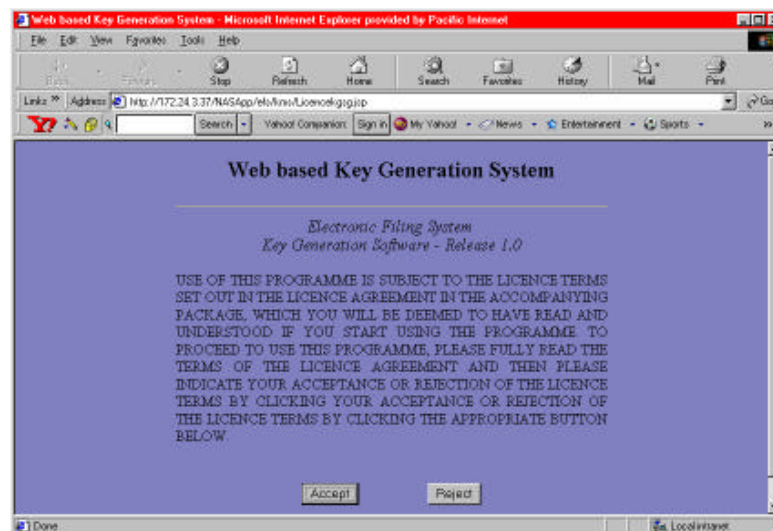


Figure 1: WKGSG - Licence Agreement

3. Click the **Accept** button to proceed. The application will terminate if the **Reject** button is clicked.
4. The system displays the **WKGSG - Login** screen (Figure 2).

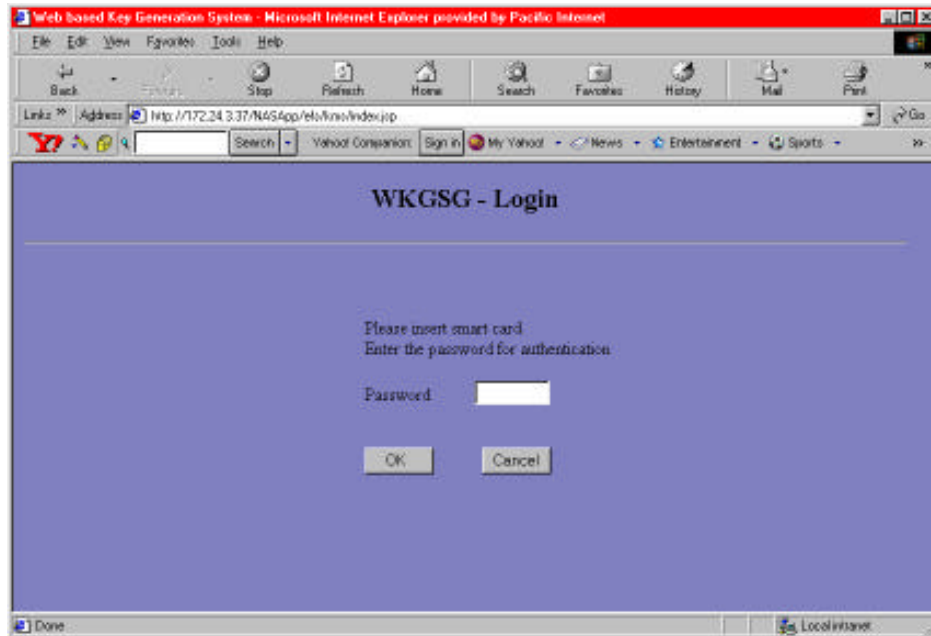


Figure 2: WKGSG - Login screen.

5. Enter the password given in the sealed mailer and click the **OK** button.

**Note:** You are given three attempts to enter the correct password. After three consecutive unsuccessful attempts, your smart card will be deactivated and you will have to submit a new certificate application.

6. On successful login, WKGSG displays the **Change Password (First Access)** screen (Figure 3).

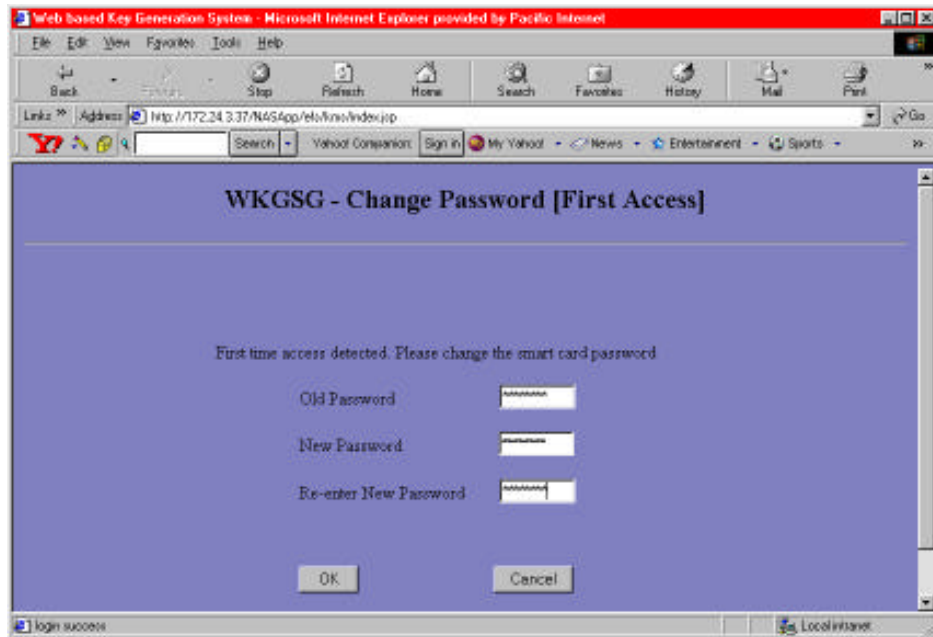


Figure 3: Change Password (First Access) screen.

7. Enter the old password (given in the mailer) and a new password of your choice (twice) and click the **OK** button.

The new password must be of 8 alphanumeric characters. Symbols and spaces are not allowed. Passwords are case sensitive – you must follow the capitals and small letters exactly the same way as you typed in the first time.

The new password entered cannot be the same as the existing password.

Upon successful verification, the system displays the message, "Password successfully changed." At this point, the system has updated the information into the smart card. Click the **OK** button to continue.

8. The system displays the **Key Generation** screen (Figure 4).

**Note:** You are given three attempts to enter the correct existing password. After three consecutive unsuccessful attempts, your smart card will be deactivated and you will have to submit a new certificate application.

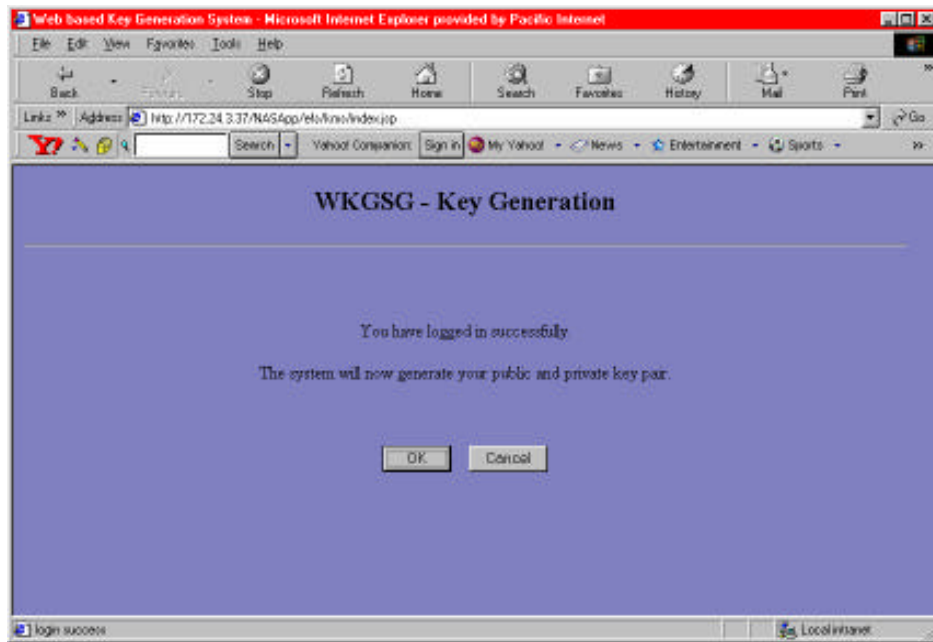


Figure 4: Key Generation screen .

9. Click the **OK** button to execute the key generation process. The application proceeds to generate the public and private keys.
10. WKGSG generates the public and private keys, and saves the key pair into the smart card.

Upon successful generation of the key pair, the system displays the message, "Key pair successfully generated. Click the **OK** button."

The application proceeds to store the public and private key pair into the user's smart card. At the same time, the system displays the message, "Saving key pair to smart card..."

11. After saving the key pair into the smart card, WKGSG displays the **WKGSG - Public Key Submission** screen (Figure 5).



Figure 5:WKGSG - Public Key Submission screen

12. Click the **OK** button.
13. WKGSG submits your public key to the CA.
14. At this point, you have successfully generated your public and private key pair, and your public key has been successfully submitted for certification. Upon successful submission, the system displays the message, "Public key successfully submitted. Please log on after two working days to receive your certificate."
15. WKGSG terminates when you click the **OK** button on this message box.

**Note:** If any error occurs in the process, WKGSG continues from the exact same process upon the next login.

## 2.2 Update Smart Card

Proceed with this process two working days after successfully generating your public and private key pair, and submitting your public key. During this time, the CA Administrator certifies your public key. You will also receive a letter notifying the successful certification.

Make sure that

- The smart card reader is properly connected

### To update your smart card with the certificate

1. Insert your smart card into the smart card reader.

**Note:** You must not remove the smart card from the smart card reader after the login procedure, until the end of the key generation session.

2. Login to the EFS application using your UserID/Password. Click on the KGSG link on the main menu in the EFS page. The **WKGSG - Licence Agreement** screen will be displayed. You are allowed to log in only after you have agreed to the terms and conditions in the agreement.

3. The system displays the WKGSG - Licence Agreement (Figure 1).

4. Click the **Accept** button to proceed.

5. The system displays the **WKGSG - Login** dialog (Figure 2).

6. Enter your smart card password, and click the **OK** button.

**Note:** You are given three attempts to enter the correct password. After three consecutive unsuccessful attempts, your smart card will be deactivated and you will have to submit a new certificate application.

7. WKGSG displays the **WKGSG - Update Smart Card** screen (Figure 6).



Figure 6: WKGSG - Update Smart Card screen

8. Click the **OK** button.
9. WKGSG retrieves your certificate from the web server, and saves it into your smart card.
10. Upon successful update and transfer, the system displays the message, "Certificate has been successfully transferred. The smart card is now activated."

With this, you have completed the Key Generation and smart card update process successfully. Your smart card is now activated.

11. Click the **OK** button and the application terminates.
12. If there is an error in this process, you can either wait for another working day and login again to update your certificate or resubmit your public key for certification. This is explained in detail in section 2.3.

## 2.3 Resubmit Public Key

WKGSG may fail to retrieve the certificate from the web server during the Update Smart Card process.

You can either resubmit the public key for certification during this session, or log in again the following working day and repeat the Update Smart Card procedure as described in section 2.2.

### To resubmit the public key

1. WKGSG displays the **Resubmit Public Key** screen (Figure 9) if the Update Smart Card process fails to update the smart card.



Figure 9: Resubmit Public Key dialog

2. Click the **OK** button if you wish to resubmit the Public Key. WKGSG automatically submits your Public Key and displays the successful Public Key submission message (please see step 14 of section 2.1.)
3. Log into KGSg after two working days and proceed with updating your smart card as described in section 2.2.

**Note:** If you decided to log in again to update your smart card, then

click the **Cancel** button. In which case the system terminates without resubmitting the Public Key.