

---

**pki Series**

# **pkiNote**

## **Quick Start Guide**

**VERSION 1.0**

**SCS.PKI.NOTE.QSG-1.0-QSG-EN 1**

---

# Terms of use

---

## Terms of Use Applicable to the User Documentation

The legal notices, disclaimers, terms of use, and other information contained herein (the "terms") apply only to the information discussed in this documentation (the "Documentation") and your use of it. These terms do not apply to or govern the use of websites controlled by Security & Communications, Inc. or its subsidiaries (collectively, "Security & Communications")

or any Security & Communications-provided products. Security & Communications products are available for purchase and subject to a separate license agreement and/or terms of use containing very different terms and conditions.

## Terms of Use and Copyright and Trademark Notices

The copyright in the Documentation is owned by Security & Communications and is protected by copyright and other intellectual property laws of the United States and other countries. You may use, print out, save on a retrieval system, and otherwise copy and distribute the Documentation solely for non-commercial use, provided that you (i) do not modify the Documentation in any way and (ii) always include Security & Communications's copyright, trademark, and other proprietary notices, as well as a link to, or print out of, the full contents of this page and its terms.

No part of the Documentation may be used in a compilation or otherwise incorporated into another work or with or into any other documentation or user manuals, or be used to create derivative works, without the express prior written permission of Security & Communications. Security & Communications reserves the right to change the terms at any time, and your continued use of the Documentation shall be deemed an acceptance of those terms.

Other company, product and service names may be trademarks or service marks of others.

© 2006 - 2013 Security & Communications, Inc. All rights reserved.

# Disclaimer

**THE DOCUMENTATION AND ANY INFORMATION AVAILABLE FROM IT MAY INCLUDE INACCURACIES OR TYPOGRAPHICAL ERRORS. Security&Communications Software MAY CHANGE THE DOCUMENTATION FROM TIME TO TIME.**

**Security&Communications Software MAKES NO REPRESENTATIONS OR WARRANTIES ABOUT THE ACCURACY OR SUITABILITY OF ANY Security&Communications Software-CONTROLLED WEBSITE, THE DOCUMENTATION AND/OR ANY PRODUCT INFORMATION.**

**Security&Communications Software-CONTROLLED WEBSITES, THE DOCUMENTATION AND ALL PRODUCT INFORMATION ARE PROVIDED "AS IS" AND Security&Communications Software DISCLAIMS ANY AND ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING BUT NOT LIMITED TO WARRANTIES OF TITLE AND THE IMPLIED WARRANTIES OF MERCHANTABILITY AND/OR FITNESS FOR A PARTICULAR PURPOSE. IN NO EVENT SHALL Security&Communications Software BE LIABLE TO YOU FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, PUNITIVE, OR CONSEQUENTIAL DAMAGES (INCLUDING BUT NOT LIMITED TO PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, LOSS OF DATA, LOSS OF PROFITS, AND/OR BUSINESS INTERRUPTIONS), ARISING OUT OF OR IN ANY WAY RELATED TO Security&Communications Software -CONTROLLED WEBSITES OR THE DOCUMENTATION, NO MATTER HOW CAUSED AND/OR WHETHER BASED ON CONTRACT, STRICT LIABILITY, NEGLIGENCE OR OTHER TORTUOUS ACTIVITY, OR ANY OTHER THEORY OF LIABILITY, EVEN IF Security&Communications Software IS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES/JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATIONS MAY NOT APPLY TO YOU.**

Copyright© 2006-2012 Security&Communications Software, Inc.  
All rights reserved.  
Security&Communications Software, Inc.®

Security & Communications Software,  
Inc.®, SE&COM™, Connection Manager™  
TransFILE™

- are registered trademarks of  
Security&Communications Software.

Microsoft®, Windows®, Windows 95®,  
Windows 98®, Windows NT®, Windows  
NT Server®, Windows 2000 Server®,  
Windows 2003 Server®, Windows XP®,  
Windows Vista®, Windows 7®, Windows  
8®

- are registered trademarks of Microsoft  
Corporation

Some parts of this guide use public information from RSA Data Security, Inc. and Microsoft Corporation.

ALBANY • NY • USA

[www.secomsoft.com](http://www.secomsoft.com)

2013

# Contents

---

<b>HOW QUICKLY TO .....</b>	<b>5</b>
INSTALLATION PROCESS .....	5
<i>install pkiNote</i> .....	5
<i>uninstall pkiNote</i> .....	5
INSTALL CERTIFICATES IN WINDOWS STORE.....	5
<i>root certificate</i> .....	5
<i>personal certificate with private key</i> .....	6
<i>friends certificates</i> .....	6
ADD CERTIFICATES TO PKINOTE MY LIST. ....	7
<i>personal certificate from file</i> .....	7
<i>personal certificate from Windows store</i> .....	7
ADD CERTIFICATES TO PKINOTE FRIENDS LIST. ....	8
<i>friends certificates from files</i> .....	8
<i>friends certificates from Windows store</i> .....	8
<i>friend certificate from text resource (import)</i> .....	8
ADD PLAIN TEXT, CIPHER, SIGNATURE AND MORE ...	8
<i>from file (drag&amp;drop)</i> .....	8
<i>from text resource (drag&amp;drop)</i> .....	9
COPY PLAIN TEXT, CIPHER, SIGNATURE AND MORE ...	9
<i>to text resource (drag&amp;drop)</i> .....	9
ENCRYPT PLAIN TEXT INTO CIPHER .....	9
<i>by password</i> .....	9
<i>by friends certificates</i> .....	10
DECRYPT PLAIN TEXT FROM CIPHER .....	10
<i>by password</i> .....	10
<i>by personal certificate</i> .....	10
SIGN PLAIN TEXT.....	10
<i>by certificate</i> .....	10
VERIFY SIGNATURE OF PLAIN TEXT .....	11
<i>by certificate</i> .....	11
EXPORT PERSONAL CERTIFICATE.....	11
<i>to text resource</i> .....	11
<i>to friends via email</i> .....	11
SEND CIPHER.....	11
<i>to friends via email</i> .....	11
SEND PLAIN TEXT WITH SIGNATURE .....	12
<i>to friends via email</i> .....	12
USE HOT KEYS.....	12

# How quickly to ...

---

## installation process...

---

### install pkiNote

---

Run installation package

**pkinoteAAA\_dd.EXE**

where:

- aaa** - current version number of pkiNote,
- dd** - language of the user interface

### uninstall pkiNote

---

To uninstall pkiNote from your PC you need to use link:

***Control Panel > Uninstall Programs (for Windows 7):***

Press **Uninstall** for removing **pkiNote** from your computer.

## install certificates in Windows store...

---

### root certificate

---

In order to install root certificate use the following procedure:

1. Double click on the certificate file (for example on **root.cer**),
2. Page with certificate properties will appear,
3. Press ***Install Certificate***,
4. You will see the first page of certificate import wizard,
5. Press **Next**,
6. You will see a page with selection of certificate store:
7. Check ***Place all certificates in the following store*** and then press ***Browse***,
8. You will see a page with a list of certificate stores,
9. Choose ***Trusted Root Certification Authorities*** and click ***OK***,
10. You will be returned to previous page with selected certificate store,
11. Press ***Next***,
12. You will see the confirmation page of certificate import wizard,
13. Press ***Finish***,
14. You will see a security message from your system,
15. Check that you have selected proper root certificate and press ***Yes***.

16. You will see successful import page.

#### Note

*You need to install the same root certificate on all computers that will be involved in information exchange.*

## personal certificate with private key

---

In order to install personal certificate please do the following:

1. Double-click on the certificate file with private key (for example, **alice.pfx**),
2. You will see the first page of certificate import wizard,
3. Press **Next**,
4. You will see a confirmation page with your selected file:
5. Press **Next**,
6. You will see a page where you will need to specify a password and additional parameters,
7. Select necessary parameters.
8. Specify the password for your private key ,

#### Note

*For demo certificates password is "test".*

9. Press **Next**,
10. You will see a page with selection of certificate store,
11. Check **Place all certificates in the following store** and then press **Browse**,
12. You will see a page with a list of certificate stores,
13. Choose **Personal** and click **OK**,
14. You will be returned to previous page with selected certificate store,
15. Press **Next**,
16. You will see the confirmation page of certificate import wizard,
17. Press **Finish**,
18. You will see successful import page.

## friends certificates

---

In order to install certificate please do the following:

1. Double-click on the certificate file (for example, **bob.cer**),

2. You will see a page with certificate properties,
3. Select **Details** tab, choose **Subject** and check name and personal data of your friend,
4. Choose **Certificate Path** tab and check that this certificate contains a proper root certificate,
5. If root certificate of issuing CA is not installed then you will see the following picture:
6. Choose **General** and press button **Install certificate**,
7. You will see the first page of certificate import wizard,
8. Press **Next**,
9. You will see a page with selection of certificate store,
10. Check **Place all certificates in the following store** and then press **Browse**,
11. You will see a page with a list of certificate stores,
12. Choose **Other People** and click **OK**,
13. You will be returned to previous page with selected certificate store,
14. Press **Next**,
15. You will see the confirmation page of certificate import wizard,
16. Press **Finish**,
17. You will see successful import page.

## add certificates to pkiNote My list...

---

### personal certificate from file

---

In order to add personal certificate to **My** list from file PFX please do the following:

1. Drag certificate file (for example, **alice.pfx**) from Windows explorer,
2. Drop certificate file on **My** tab of certificates list,
3. Enter password and confirm in another field ,

#### Note

*For demo certificates password is "test".*

4. Personal certificate will be added to **My** list.

### personal certificate from Windows store

---

In order to add personal certificate from Windows to **My** list please do the following:

1. Press **Ctrl-T**,

2. Drag personal certificate from Windows store certificates list,
3. Drop certificate on **My** tab,
4. Personal certificate will be added to **My** list.

## add certificates to pkiNote Friends list...

---

### friends certificates from files

---

In order to add friends certificate to Friends list from CER files please do the following:

1. Press **Ctrl+1**,
2. In certificates list select **Friends** tab,
3. Drag certificates CER files from Windows explorer,
4. Drop certificates files on **Friends** tab of certificates list,
5. Friends certificates will be added to **Friends** list.

### friends certificates from Windows store

---

In order to add friends certificates from Windows to Friends list please do the following:

1. Press Ctrl-J,
2. Select certificate in list,
3. Drag selected certificates from Windows store,
4. Drop certificates on **Friends** tab,
5. Selected certificates will be added to Friends list.

### friend certificate from text resource (import)

---

In order to add friend certificate to Friends list from text resource please do the following:

1. Press **Ctrl+1**,
2. Select certificate in text resource,
3. Drag certificate in text resource from,
4. Drop certificate on main text window of pkiNote,
5. Click **Yes**, If you want to install this certificate to Windows store,
6. Imported friend certificate will be added to **Friends** list.

## add plain text, cipher, signature and more ...

---

### from file (drag&drop)

---

In order to add plain text, cipher, signature and more from file please do the following:

1. Drag file in Windows Explorer,



2. Drop file on main text window of pkiNote,

### Note

*In this version you can drag&drop contents only from TXT, HTM, HTML. files*

3. Content will be added to Plain object.

## from text resource (drag&drop)

---

In order to add plain text, cipher, signature and more from text resource please do the following:

1. Select plain text, cipher text, signature, certificate or session keys in resource,
2. Drag selected object,
3. Drop selected object on main text window of pkiNote,
4. Selected object will be added to appropriate object.

## copy plain text, cipher, signature and more ...

---

### to text resource (drag&drop)

---

In order to copy plain text, cipher, signature and more from main text window to text resource please do the following:

1. Select required object ,
2. View selected object in main text window,
3. Drag object in main window,
4. Drop object on text resource,
5. Selected object will be copy to text resource.

## encrypt plain text into cipher

---

### by password

---

In order to encrypt plain text into cipher by password please do the following:

1. Add plain text (see *add plain text, cipher, signature and more ...*),
2. Press **Ctrl+2**,
3. Enter password in **Encryption password** field,
4. Press gray image of key,
5. Press **Ctrl+E**,
6. Encrypted plain text will be copy to **Cipher** object.

## by friends certificates

---

In order to encrypt plain text into cipher by friends certificates please do the following:

1. Add plain text (see *add plain text, cipher, signature and more ...*),
2. Press **Ctrl+1**,
3. Add friends certificates (see *add certificates to pkiNote Friends list...*),
4. Press button **New** in **Encryption session key**,
5. Press **Ctrl+E**,
6. Click **Ok** in message about session keys,
7. Encrypted plain text will be copy to **Cipher** object,
8. Encrypted session keys will by copy to **Session Keys** object.

## decrypt plain text from cipher

---

### by password

---

In order to decrypt plain text from cipher by password please do the following:

1. Add cipher (see *add plain text, cipher, signature and more ...*),
2. CIPHERRJN:3KarqOH4DKzyeZXCTHrPaYBqr8ljs3e813v871/2lwU=Press **Ctrl+2**,
3. Enter password in **Decryption password** field,
4. Press gray image of key,
5. Press **Ctrl+D**,
6. Successfully decrypted plain text will be copy to **Plain** object.

### by personal certificate

---

In order to decrypt plain text from cipher by personal certificate please do the following:

1. Press **Ctrl+1**,
2. Add encrypted session keys (*add plain text, cipher, signature and more ...*),
3. If encrypted session key successfully decoded key image in **Decode automatically** will be green,
4. Add cipher text (see *add plain text, cipher, signature and more ...*),
5. Press **Ctrl+D**,
6. Successfully decrypted plain text will be copy to **Plain** object,

## sign plain text

---

### by certificate

---

In order to sign plain text by certificates please do the following:

1. Add personal certificate (see *add certificates to pkiNote My list...*),
2. Add plain text (see *add plain text, cipher, signature and more ...*),

3. Press **Ctrl+W**,
4. Signature of plain text will be copy to **Signature** object.

## verify signature of plain text

---

### by certificate

---

In order to verify signature of plain text by friend certificate please do the following:

1. Add friend certificate (see *add certificates to pkiNote Friends list...*),
2. Add plain text (see *add plain text, cipher, signature and more ...*),
3. Add signature (see *add plain text, cipher, signature and more ...*),
4. Press **Ctrl+R**,
5. Signature of plain text will be verified.

## export personal certificate

---

### to text resource

---

In order to export personal certificate to text resource please do the following:

1. Add personal certificate (see *add certificates to pkiNote My list...*),
2. Press **Ctrl+Q**,
3. Personal certificate will be copy to **Certificate** object,
4. Drag Certificate object,
5. Drop Certificate object to text resource.

### to friends via email

---

In order to export personal certificate and send to friends via email please do the following:

1. Add personal certificate (see *add certificates to pkiNote My list...*),
2. Add friends certificates (see *add certificates to pkiNote Friends list...*),
3. Press **F8**,
4. Email (MAPI) message to friends from Friends list will be created with exported personal certificate.

## send cipher

---

### to friends via email

---

In order to encrypt plain text and send cipher to friends via email please do the following:

1. Add friends certificates (see *add certificates to pkiNote Friends list...*),
2. Encrypt plain text (see *encrypt plain text into cipher-> by friends certificates*),

3. Select **Cipher** object,
4. Drag **Cipher** object,
5. Drop **Cipher** object on image **Email** on screen bottom,
6. Email (MAPI) message to friends from **Friends** list will be created with encrypted session keys and cipher,

## send plain text with signature

---

### to friends via email

---

In order to sign plain text and send plain text with signature to friends via email please do the following:

1. Add friends certificates (see *add certificates to pkiNote Friends list...*),
2. Sign plain text (see *sign plain text*),
3. Select **Signature** object,
4. Drag **Signature** object,
5. Drop **Signature** object on image **Email** on screen bottom,
6. Email (MAPI) message to friends from **Friends** list will be created with plain text and signature.

## use hot keys

---

This hot key you can use to perform operations:

Hot keys	Operation description
<b>Ctrl+N</b>	Create new file with empty content
<b>Ctrl+O</b>	Open file and load content
<b>Ctrl+S</b>	Save content to file
<b>Ctrl+P</b>	Print content
<b>Ctrl+Z</b>	Undo edition
<b>Ctrl+X</b>	Cut content in clipboard
<b>Ctrl+C</b>	Copy content in clipboard
<b>Ctrl+V</b>	Paste clipboard in content
<b>Del</b>	Delete selected part of content
<b>Ctrl+F</b>	Find substring of content
<b>F3</b>	Find next substring of content
<b>Ctrl+H</b>	Replace substring in content to another substring
<b>Ctrl+G</b>	Go to line number of content
<b>Ctrl+M</b>	Change font

<b>Ctrl+E</b>	Encrypt plain text
<b>Ctrl+D</b>	Decrypt cipher text
<b>Ctrl+W</b>	Sign plain text
<b>Ctrl+R</b>	Verifysignature of plain text
<b>Ctrl+T</b>	Add or change personal (My) certificate from store to list
<b>Ctrl+Y</b>	Remove personal (My) certificate from list
<b>Ctrl+U</b>	View personal (My) certificate properties
<b>Ctrl+Q</b>	Export personal (My) certificate
<b>F8</b>	Send personal (My) certificate via email
<b>Ctrl+J</b>	Add friend certificate from store to list
<b>Ctrl+K</b>	Remove selected friend certificate from list
<b>F12</b>	Remove all friends certificates from list
<b>Ctrl+L</b>	View selected friend certificate properties
<b>Ctrl+1</b>	Create keys from certificates
<b>Ctrl+2</b>	Create keys from passwords
<b>Ctrl+B</b>	Export session keys
<b>Ctrl+I</b>	Import session keys
<b>F1</b>	View user guide
<b>F2</b>	View quick start guide