

Haachtsesteenweg 1442 1130 Brussels Belgium

DEP Documentation

RSA Key Import In Keytable User Manual

Version Management Report						
Version	Name(s)	Date	Comments			
01.00	David Lheureux	17/08/2006	First version			
01.01	David Lheureux	17/08/2006	After review			
01.02	EGS	10/07/2009	Support the import of an RSA key encrypted with an AES transport key.			
01.03	David Lheureux	15/10/2010	Review document and use the Atos Worldline logo.			
04.00	Anna Papayan	05/04/2011	Change the template into Atos Worldline, minor changes.			

CONFIDENTIALITY

The information in this document is confidential and shall not be disclosed to any third party in whole or in part without the prior written consent of Atos Worldline S.A./N.V.

COPYRIGHT

The information in this document is subject to change without notice and shall not be construed as a commitment by Atos Worldline S.A./N.V.

The content of this document, including but not limited to trademarks, designs, logos, text, images, is the property of Atos Worldline S.A/N.V. and is protected by the Belgian Act of 30.06.1994 related to author's right and by the other applicable Acts.

The contents of this document must not be reproduced in any form whatsoever, by or on behalf of third parties, without the prior written consent of Atos Worldline S.A./N.V.

Except with respect to the limited license to download and print certain material from this document for non-commercial and personal use only, nothing contained in this document shall grant any license or right to use any of Atos Worldline S.A./N.V.'s proprietary material.

LEGAL DISCLAIMER

While Atos Worldline S.A./N.V. has made every attempt to ensure that the information contained in this document is correct, Atos Worldline S.A./N.V. does not provide any legal or commercial warranty on the document that is described in this specification. The technology is thus provided "as is" without warranties of any kind, expressed or implied, included those of merchantability and fitness for a particular purpose. Atos Worldline S.A./N.V. does not warrant or assume any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, product or process disclosed.

To the fullest extent permitted under applicable law, neither Atos Worldline S.A./N.V. nor its affiliates, directors, employees and agents shall be liable to any party for any damages that might result from the use of the technology as described in this document (including without limitation direct, indirect, incidental, special, consequential and punitive damages, lost profits).

JURISDICTION AND APPLICABLE LAW

These terms shall be governed by and construed in accordance with the laws of Belgium. You irrevocably consent to the jurisdiction of the courts located in Brussels for any action arising from or related to the use of this document.

sa Atos Worldline nv – Chaussée de Haecht 1442 Haachtsesteenweg B-1130 Bruxelles-Brussel - Belgium RPM-RPR Bruxelles-Brussel - TVA-BTW BE 0418.547.872

TABLE OF CONTENTS

1.	SC	OPE OF THE DOCUMENT	5
	1.1.	References	5
	1.2.	CONTACTING ATOS WORLDLINE	5
2.	PU	RPOSE OF RSA KEY IMPORT IN KEYTABLE PROGRAM	6
3.	USI	E OF RSA KEY IMPORT IN KEYTABLE	6
	3.1.	PREREQUISITES	6
	3.2.	START-UP	6
	3.3.	DESCRIPTION	7
	3.4.	COMMUNICATION	7
	3.5.	HOW TO IMPORT AN RSA KEY	8
	3.6.	Errors during execution	10
	3.6.	1. Validation of input data	
	3.6.	2. Validation of the DEP Crypto Module	10
	3.6.	3. Error code from the DEP Crypto Module	11
4.	AN	NEX A: INSTALLATION PROCEDURE	13
5.	AN	NEX B: NOTATIONS	

1. SCOPE OF THE DOCUMENT

This document describes how to import RSA Keys into the DEP Crypto Module (RSA Key Pair and RSA Public Key) using the *RSA Key Import In Keytable* program.

The document doesn't explain the functionalities of the DEP libraries on which this program is based.

1.1. REFERENCES

This document contains references to other documents about the DEP. This paragraph gives a list of all the documents referred to:

- DEP Host Interface Protocol
- DEP/NMS User Manual
- DEP/Linux User Manual
- DEP/T6 Owner Manual

There are no references made to the following documents, but they could be useful to understand this document:

- PKI Library for DEP Reference DFS Manual
- DEP Introduction to DEP
- DEP General Architecture
- DEP Glossary
- DEP RSA Key Generation User Manual

1.2. CONTACTING ATOS WORLDLINE

You can visit *Atos Worldline* on the World Wide Web to find out about new products and about various other fields of interest.

URL: <u>www.atosworldline.com</u>.

For the documentation visit http://www.banksys.com web page.

For support on issues related to DEP, customers, partners, resellers, and distributors can send an email to the DEP Hotline: mailto:dephotline-atosworldline@atosorigin.com.

2. PURPOSE OF RSA KEY IMPORT IN KEYTABLE PROGRAM

The purpose of this program is to import RSA Keys into the DEP Crypto Module (RSA Key Pair and RSA Public Key) and put it in a specific TAG in the DEP Keytable.

The program is intended to be used on a PC (running on Microsoft Windows 2000, Windows XP and Windows Vista) that is connected to a DEP Platform loaded with a DEP Application Software that can import and store RSA Keys. It also can be added as a plug-in in *DEP/NMS* application.

3. USE OF RSA KEY IMPORT IN KEYTABLE

The installation procedure is reported to the Annex A on page 13.

3.1. PREREQUISITES

- The DEP Crypto Module must be unlocked;
- A valid DEP Application Software should be loaded on DEP Crypto Module;
- A DEP Application Software that supports the import of RSA Keys should be loaded on DEP Crypto Module;
- The **K_PKI_RSA_TRANSPORT_KEY** or the **K_PKI_RSA_TK_AES** transport key should be loaded in DEP Crypto Module depending on the export method to be chosen (DES or AES);
- The CAP_STD_SAVE_KEYS capability should be loaded in DEP Crypto Module;
- To use the RSA Key Import In Keytable application as a DEP/NMS plug-in, the USB License Dongle must be present.

3.2. START-UP

The RSA Key Import In Keytable program can be launched by executing:

C:\Program Files\Atos Worldline\DEP_NMS_PlugIns\RSA Key Import In Keytable\RSA_KeyImportInKeytable.exe

This is the default path. Another path can also be defined during the installation (paragraph 4 on page 13).

The application can also be launched directly from the *DEP/NMS* program. Select the appropriate DEP Crypto Module and run the *RSA_KeyImportInKeytable* plug-in from the **Plug Ins** menu.

± DEP/NMS C:\192.168.0.19.cfg							
File Edit View DEP Platform	n - DEP Cry	ypto Module – Too	ols	Plug Ins	Help		
🗅 😅 🖬 🞒 🎥 💷 💷 🐺 🚑 🥕 🏸			Add Plug In				
Platform symbolic name	Security	Platform status	Tr	Organize Plug Ins			iame
- 🗐 192.168.0.19.cfg				NCR_S	SelfSignedCerti	ficate	
- 🔜 192.168.0.172	-8	Unlocked	OI RSA_KeyImportInKeytable		/table		
- Module 1				Import	ExportKeys		
Module 2				CTAP_	CertificateGen	eration	
				RSA_KeyGeneration			
			—	_			-

Before starting the application, the communication must be defined (paragraph 3.4 on page 7).

3.3. DESCRIPTION

Once the RSA Key Import In Keytable program is started, the following window is opened:

🗝 RSA Key Import In Keytable	
Eile Help	
Key Tag for the Imported RSA Key:	<u>^</u>
Import RSA Key Pair or RSA Public Key from File.	
RSA Key File: Browse	
Import method	
Import using DEC Transport Koy	
 Import using AES Transport Key 	
Instance Byte: 00 ('00' by default)	
C Import RSA Public Key from Input.	
Public Evonent: (Decimal Value)	
Modulus:	
	T
	Import RSA Key
DEP Platform 192.168.0.19 - Not Connected DEP Crypto Module numbe	r 01

A menu at the top of the window allows to have a look at the program version (and also contact the DEP Hotline), the help files or to exit.

The *Input* section contains the list of parameters needed to import an RSA Key (see paragraph 3.5 on page 8). The *Output* section (blank part) will log the operations and their results.

3.4. COMMUNICATION

If the application is launched by the DEP/NMS the communication is automatically set by the *DEP/NMS* program.

If the application is used as stand-alone application, the user should set the general parameters and the connection settings in the *RSA_KeyImportInKeytable.ini* configuration file.

🜌 RSA_KeyImportInKeytable.ini - Notepad	- 🗆 🗵
File Edit Format Help	
[GeneralParameters] NbofDesiredConnections=1 [Connection_0] Address=172.24.14.249 Port=1000 Timeout=180000 TimeoutConnection=5000 Module=0101 LSBMSBmode=LSB LSBMSBLength=4 DEPMagicNumber=FE DEPVersionNumber=30	×

- *NbOfDesiredConnections* must be set to '1'.
- *Address* represents the IP address of the target DEP Platform.
- *Port* represents the TCP/IP port used for the communication with the DEP Platform.
- *TimeOut* represents in milliseconds the maximum waiting time for the response from the DEP Crypto Module.
- *TimeOutConnection* represents in milliseconds the maximum waiting time for establishing a connection.
- *Module* represents the DEP Crypto Module used to import an RSA Key: the first byte will be always '01' and the second byte defines the target module: '01' to '04'.
- The four last parameters are described in the DEP Documentation (*DEP Host Interface Protocol*)

3.5. HOW TO IMPORT AN RSA KEY

There are two methods to import an RSA Key into the keytable of the DEP Crypto Module (selected by radio buttons):

- Import an RSA Key Pair (.RSA) or an RSA Public Key (.PUB) from file. These files are generated by the *RSA Key Generation* program (refer to the *RSA Key Generation User Manual* for more information).
- Import an RSA Public key coming from the input of the user.

In both cases the Key Tag is mandatory.

If the *Import RSA Key Pair or RSA Public key from file* case is selected in the dialogue box, the valid ".RSA" or ".PUB" file should be selected by the user. Click the **Browse...** button and select the appropriate file.

ile Help nput Key Tag for the Imported RSA Key: 04250799 Import RSA Key Pair or RSA Public Key from File. RSA Key File: D:\L2048E00065537\20090720122148734.RSA Browse Import method Import using DES Transport Key Import using DES Transport Key Import using AES Transport Key Import using AES Transport Key Import RSA Public Key from Input. Public Exponent: Moddutus: Decimal Value Module Validation of the DEP Cupto Module. Decimal Value Moddutus: Decimal Value Moddutus: Decimal Value Moddutus: Decimal Value Module Validation of the DEP Cupto Module. Decimal Value Moddutus: Decimal Value Moddutus: Decimal Value Module Validation of the DEP Cupto Module. Decimal Value Module Validation of the DEP Cupto Module. Decimal Value Module Validation of the DEP Cupto Module. Decimal Value Module Validation of the DEP Cupto Module. Decimal Value Module Validation of the DEP Cupto Module. Decimal Value Module Validation of the DEP Cupto Module. Decimal Value Module Validation of the DEP Cupto Module. Decimal Value Module Validation of the DEP Cupto Module. Decimal Value Module Validation of the DEP Cupto Module. Decimal Value Module Validation of the DEP Cupto Module. Decimal Value Module Validation of the DEP Cupto Module. Decimal Value Module Validation of the DEP Cupto Module. Decimal Value Module Validation of the DEP Cupto Module. Decimal Value Module Validation of the DEP Cupto Module. Decimal Value Module Validation of the DEP Cupto Module. Decimal Value Module Validation of the DEP Cupto Module. Decimal Value Module Validation of the DEP Cupto Module Validation of the DEP Cupto Module. Decimal Validation of the DEP Cupto Module Validati			
put Output Key Tag for the Imported RSA Key: 04250799 Import RSA Key Pair or RSA Public Key from File. Walidation of input data RSA Key File: D:\L2048E00065537\20090720122148734.RSA Browse Import method Send call to the DEP Crypto Module Import using AES Transport Key Send call to the DEP Crypto Module Instance Byte: 00 (100' by default) Import RSA Public Key from Input. Public Exponent: (Decimal/Value) Modulus: (Decimal/Value) (Decimal/Value)	e Help		
	Help put Key Tag for the Imported RSA Key: 04250739 Import RSA Key Pair or RSA Public Key from File. RSA Key File: D:\L2048E00065537\20090720122148734.RSA Browse Import method Import using DES Transport Key Instance Byte: 00 ('00' by default) Import RSA Public Key from Input. Public Exponent: Decimal Value Modulue:	Dutput Validation of input data Validation of input data succeeded. Import an RSA Key Pair in the Tag 04250799 The RSA File is valid. Send call to the DEP Crypto Module Receive answer from the DEP Crypto Module Valid answer received. The key is written in the Key Table of the DEP Crypto Module.	

If the *Import RSA Public Key from Input* is selected, then the user must fill in the *Public Exponent* and *Modulus* fields.

🗝 RSA Key Import In Keytable	
<u>File</u> <u>H</u> elp	
	Output
Key Tag for the Imported RSA Key: 04250799	Validation of input data Validation of input data succeeded.
O Import RSA Key Pair or RSA Public Key from File.	Import an RSA Public Key in the Tag 04250799
RSA Key File: Browse	Send call to the DEP Crypto Module Receive answer from the DEP Crypto Module Valid answer received.
C Import using DES Transport Key	The key is written in the Key Table of the DEP Crypto Module.
Import using AES Transport Key	
Instance Byte: 00 ('00' by default)	
Import RSA Public Key from Input.	
Public Exponent: 65537 (Decimal Value)	
Modulus: BAC458C34CC3F0AE 4ABADF5B3CC43F2A53501AA8044F2D	
	Import RSA Key
DEP Platform 192.168.0.19 - Not Connected DEP Crypto Module number	01

Description/format of the parameters:

Field Name	Length	Description	Format
Key Tag	4	This data contains the tag of an RSA	b
		key in the keytable of the DEP	
		Crypto Module.	
RSA Key	/	This field contains the file name of	/
File		the RSA Key to import (.RSA or	
		.PUB).	
Instance	1	Instance of AES transport key to be	h2
Byte		used in import	
Public	5	Public exponent for the RSA Key to	n10
Exponent		generate. The maximum value is	
		4294967295 (=FFFFFFFFF _{hex}).	

Modulus	Max 512	Modulus for the RSA Public Key to	b
		import. (RSA 4096 bits depending on	
		the hardware of the DEP Crypto	
		Module).	

User must select the importing method to be used for import of RSA Key Pair. If *Import using DES Transport key* is selected, then the private part of RSA Key Pair will be decrypted by using DES transport key. If *Import using AES Transport key* is selected, then the private part of RSA Key Pair will be decrypted by using the appropriate instance of AES transport key.

When the user clicks the **Import RSA Key** the TCP/IP connection to the DEP Crypto Module is established and the key is imported.

The right panel shows the progress of the import:

- The validation of the input data,
- The validation of the file (in case of import from file only),
- The status of the call sent to the DEP Crypto Module,
- The confirmation of the writing of the key,
- The possible errors.

3.6. ERRORS DURING EXECUTION

3.6.1. Validation of input data

Before sending the call to the DEP Crypto Module some verifications are made and messages are displayed.

For example:



Selecting the **OK** button sets the focus to the erroneous field for correction.

3.6.2. Validation of the DEP Crypto Module

After the input validation, the application performs a DEP Crypto Module validation: The following conditions will be checked:

- If the DEP Crypto Module is on-line/unlocked;
- If the DEP Crypto Module contains a valid DEP Application Software;
- If the DEP Application Software is able to import RSA Keys;

- If the K_PKI_RSA_TRANSPORT_KEY (DES transport key) or the K_PKI_RSA_TK_AES (AES transport key) key is loaded in the DEP Crypto Module.
- If the CAP_STD_SAVE_KEYS capability is loaded in the DEP Crypto Module.

If one of the verification failed, a warning window is displayed:

🗝 Warni	ing X
	The DEP Crypto Module doesn't contain the capability CAP_STD_SAVE_KEYS(05000000). Please load the capability.
	(OK]

All warning windows disappear automatically when the problem is solved. For example: when the correct capability is loaded or when the DEP Crypto Module is set on-line/unlocked.

🗝 Warnii	ng X
⚠	The DEP Crypto Module is in OFF LINE/LOCKED mode. Please select ON LINE/UNLOCK mode.
	ΟΚ

The user can also click on the **OK** button, solve the problem and click again on **Import RSA Key** button.

3.6.3. Error code from the DEP Crypto Module

After all verifications are done successfully, a call is sent to the DEP Crypto Module. When no problem occurs the RSA Key is imported into the key table, otherwise an error message is returned.

For example:

Error		×
8	The field "Key Tag" doesn't contain a valid tag for an RSA Key. See the Software DFS of the loaded DEP Application Software for having all valid RSA Ke	y Tags and try again.
	<u>(ОК</u>)	
	Error	
	FF0225000003002800 The imported key (RSA key or ECC key) is corrupted.	
	(OK	



4. ANNEX A: INSTALLATION PROCEDURE

An installation procedure exists for the RSA Key Import In Keytable program. It is a wizard-driven procedure that lets you to install the RSA Key Import In Keytable program. To begin the installation wizard, execute the **setup.exe**.



Click **Next** to continue.

Read and accept the License Agreement.

🔂 RSA Key Import In Keytable - InstallShield Wizard	×			
License Agreement Please read the following license agreement carefully.				
CONFIDENTIALITY The information in this software is confidential and shall not be disclosed to any third party in whole or in part without the prior written consent of Atos Worldline S.A./N.V. COPYRIGHT The information in this software is subject to change without notice and shall not be construed as a commitment by Atos Worldline S.A./N.V. The content of this software, including but not limited to trademarks, designs, logos, text, images, is the property of Atos Worldline S.A/N.V. and is protected by the Belgian Act of 30.06.1994 related to author's right and by the				
 I accept the terms in the license agreement I do not accept the terms in the license agreement 				
InstallShield < <u>B</u> ack <u>N</u> ext > Cancel				

Click **Next** to continue.

The **Destination Folder** window allows defining the path where the application is installed. It is recommended to use the default path, yet you can specify a different folder by clicking **Change...** and selecting the desired folder for the installation.

🙀 RSA Key Import In Keytable - InstallShield Wizard 🛛 🗙				
Destination Folder Click Next to install to this folder, or click Change to install to a different folder.				
	Install RSA Key Import In Keytable to: C:\Program Files\Atos Worldline\DEP_NMS_PlugIns\RSA Key]		
InstallShield -	< <u>B</u> ack <u>Next</u> > Cancel			

Click the **Next** button.

Click the **Install** button to start an installation process. If you want to return to the previous screen, press **Back** or if you want to abort the procedure, click **Cancel**.

🙀 RSA Key Import In Keytable - InstallShield Wizard	×
Ready to Install the Program The wizard is ready to begin installation.	
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.	
Current Settings:	
Setup Type: Destination Folder: C:\Program Files\Atos Worldline\DEP_NMS_PlugIns\RSA Key Import In Keytable\	
User Information:	
Name: USER	
Company:	
InstallShield	
< <u>B</u> ack <u>Install</u> Cancel	

Once you have confirmed the installation options, the actual installation starts.

Click **Finish** to exit the installation procedure.



5. ANNEX B: NOTATIONS

The following abbreviations are used in this document.

b	Binary
n	Numeric
h	Hexadecimal