SafeSign Identity Client Minidriver

UZI-pas 3 QSCD Activation

Table of Contents

Table of Figures

Warning Notice

All information herein is either public information or is the property of and owned solely by A.E.T. Europe B.V. who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

This information is subject to change as A.E.T. Europe B.V. reserves the right, without notice, to make changes to its products, as progress in engineering or manufacturing methods or circumstances warrant.

Installation and use of A.E.T. Europe B.V. products are subject to your acceptance of the terms and conditions set out in the license Agreement that accompanies each product. Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/ or industrial property rights of or concerning any of A.E.T. Europe B.V. information.

Cryptographic products are subject to export and import restrictions. You are required to obtain the appropriate government licenses prior to shipping this Product.

The information contained in this document is provided “AS IS” without any warranty of any kind. Unless otherwise expressly agreed in writing, A.E.T. Europe B.V. makes no warranty as to the value or accuracy of information contained herein. The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, A.E.T. Europe B.V. reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

A.E.T. EUROPE B.V. HEREBY DISCLAIMS ALL WARRANTIES AND CONDITIONS WITH REGARD TO THE INFORMATION CONTAINED HEREIN, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL A.E.T. EUROPE B.V. BE LIABLE, WHETHER IN CONTRACT, TORT OR OTHERWISE, FOR ANY INDIRECT, SPECIAL OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER INCLUDING BUT NOT LIMITED TO DAMAGES RESULTING FROM LOSS OF USE, DATA, PROFITS, REVENUES, OR CUSTOMERS, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF INFORMATION CONTAINED IN THIS DOCUMENT.

SafeSign IC is a trademark of A.E.T. Europe B.V. All A.E.T. Europe B.V. product names are trademarks of A.E.T. Europe B.V. All other product and company names are trademarks or registered trademarks of their respective owners.

Credit Information:

“This product includes cryptographic software written by Eric A. Young (eay@cryptsoft.com). “

“This product includes software written by Tim J. Hudson (tjh@cryptsoft.com). “

Document Information

Document ID: SafeSign IC Minidriver Version 3.6 Activate UZI-pas 3 QSCD

Project Information: SafeSign IC Release Documentation

Document revision history:

Version	Date	Author	Changes
1.0	17 September 2020	Drs C.M. van Houten	First edition for SafeSign IC Minidriver Version 3.6 for Windows, release 3.6.0.0-AET.000
1.1	10 November 2020	Drs C.M. van Houten	Edited for SafeSign IC Minidriver Version 3.6 for Windows, release 3.6.0.0-AET.000
2.0	22 September 2021	Drs C.M. van Houten	First edition for SafeSign IC Minidriver Version 3.7 for Windows, release 3.7.0.0-AET.000

Document Approval

Version	Date	Name	Function
1.0	17 September 2020	B. Smid MBT	Chief Development Officer
1.1	10 November 2020	B. Smid MBT	Chief Development Officer
2.0	22 September 2021	B. Smid MBT	Chief Development Officer

WE RESERVE THE RIGHT TO CHANGE SPECIFICATIONS WITHOUT NOTICE

About the Product

This competent all-rounder in terms of strong authentication, integration and compatibility gives you complete freedom and flexibility. Once rolled out, SafeSign Identity Client (IC) serves as the perfect guard for IT security and enables unlimited possibilities for securing your IT infrastructure.

SafeSign IC offers the most comprehensive support available on the market for (card) operating systems, smart cards, USB tokens, languages and functions. This means you have sustainable and permanent freedom of choice when it comes to manufacturer independence.

SafeSign IC enforces two- or multi factor authentication/logon to the network, client PC or application, requiring the end user to have both the USB token or smart card (something you have) and a Personal Identity Number (something you know). USB tokens and smart cards are physically and logically tamper-resistant, ensuring that the end user’s digital credentials can not be copied, modified or shared. Authentication based on smart cards or USB tokens provides the highest degree of security.

SafeSign IC is available for both fixed and mobile devices like desktops, servers, laptops, tablets and smart phones. SafeSign IC is also found in Thin Clients, printers or any other devices requiring authentication.

1 QSCD Card Activation

In accordance with the (European) eIDAS Regulation and related standards for cryptographic modules, the legitimate user / signatory of a Qualified Signature Creation Device (QSCD) is reponsible for activating the card (keys), i.e. to change the state of the card (keys) from non-operational to operational.

When a QSCD is inserted in the smart card reader, the SafeSign IC middleware will enable the user to activate the card, based on the presence of the Common Criteria (CC) certified SafeSign IC applet and the card specific ATR. If these conditions are met, the Token menu of the SafeSign IC Token Administration Utility will display the option ‘Activate Card’.

📌 Note that the activation process for particular cards may differ.

2 UZI-pas 3 QSCD

Unlike the UZI-pas 2 card, the UZI-pas 3 card needs to be activated before it can be used. This is due to the fact that the UZI-pas 3 card is a QSCD (Qualified Signature Creation Device), that can be used for creating qualified digital signatures. Before the UZI-pas 3 card is valid and can be used, the keys on the card will have to be activated, i.e. made operational.

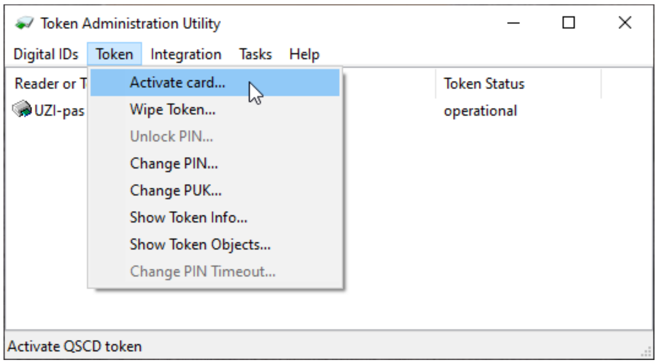
From SafeSign IC Minidriver Version 3.5.6.1 onwards, the SafeSign IC Token Administration Utility offers users of an UZI-pas 3 QSCD to activate their card.

> Note that activating the UZI-pas 3 card requires the user to authenticate to the card by entering the correct PIN, as included in the PIN mailer the user has received, there is no separate or special activation code required.

2.1 Activate UZI-pas 3

When an UZI-pas 3 is inserted in the smart card reader, the SafeSign IC middleware will enable the user to activate the card, based on the presence of the CC certified SafeSign IC applet and the specific UZI-pas 3 ATR.

1 If these requirements are met, the Token menu of the SafeSign IC Token Administration Utility will display the option ‘Activate card’:

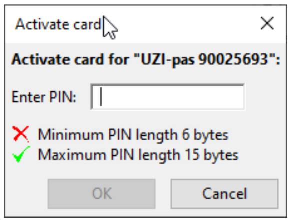


Reader or T | Token Status
UZI-pas | operational

Activate QSCD token

Figure 1: Token Administration Utility: Activate card

2 If this option is selected, the *Activate card* dialog will be displayed:



Activate card for "UZI-pas 90025693":

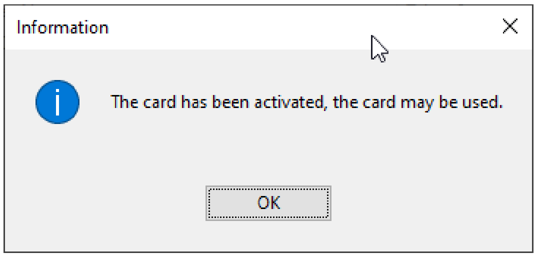
Enter PIN:

✗ Minimum PIN length 6 bytes
✓ Maximum PIN length 15 bytes

Figure 2: Activate card

This dialog will ask the user the enter the PIN (i.e. to authenticate with his PIN) for the UZI-pas 3 card, which is included in the PIN mailer the user has received.

3 After entering the correct PIN and clicking **OK**, the card will be successfully activated:



Information

The card has been activated, the card may be used.

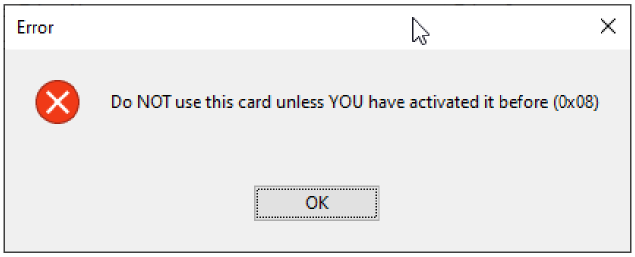
Figure 3: Activate card: Information

The keys on the card are activated now and ready to be used.

2.2 Activated UZI-pas 3

When the UZI-pas 3 has been activated, the card and its keys can be used in PKI applications.

However, if the card is already activated and the user tries to activate his card for the second time (or subsequent times), the following message will be displayed:



Error

Do NOT use this card unless YOU have activated it before (0x08)

Figure 4: Activate card: Do NOT use this card unless YOU have activated it before

➡ It is important that activating the card is a one-time and conscious action of the user. If the user tries to activate the card and gets the error message above, and he did not activate the card himself / herself before, he should verify why this is so or who activated his card and <u>**not**</u> use it.

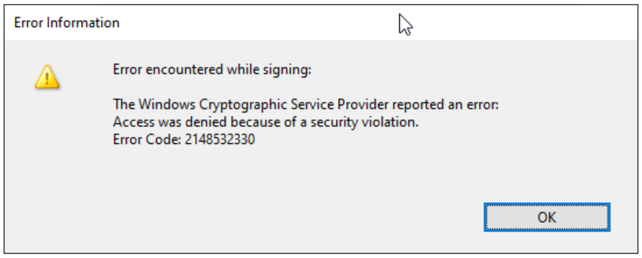
3 Non-Activated UZI-pas 3

3.1 UZI-pas 3 not (yet) activated

If the user does not activate the card, the keys on the card cannot be used, although the card does have a valid PIN and the user enters it correctly. This means that if the user tries to use the card with PKI applications before it is activated, an error message will be displayed.

3.1.1 Document signing

In Adobe Reader DC, the following error message will appear when signing a document (after the certificate for signing was selected and the correct PIN was entered):



Error Information

Error encountered while signing:

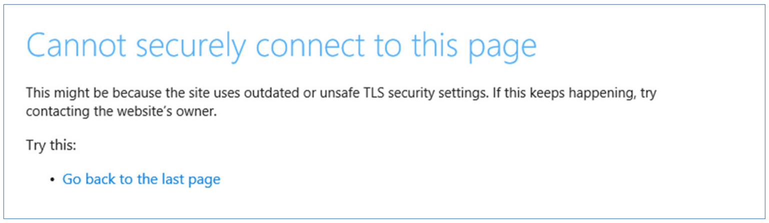
The Windows Cryptographic Service Provider reported an error:
Access was denied because of a security violation.
Error Code: 2148532330

Figure 5: Adobe Reader: Error Information

3.1.2 Web authentication

In a web browser, when trying to authenticate to a secure (IIS) website with a card that has not been activated yet (after the certificate for signing was selected and the correct PIN was entered), you will get an error message.

Internet Explorer:



Cannot securely connect to this page

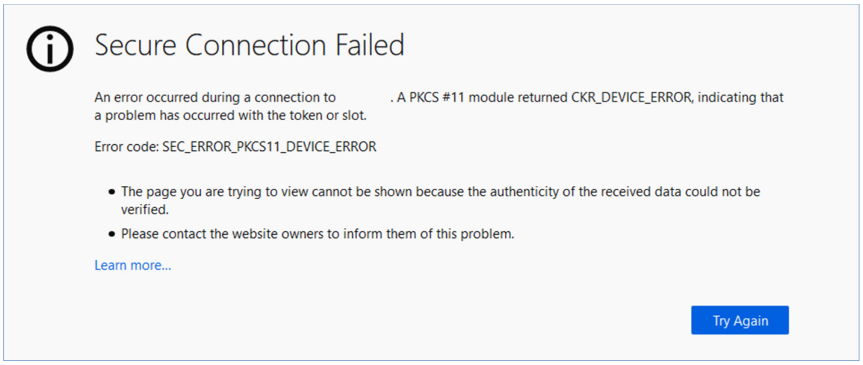
This might be because the site uses outdated or unsafe TLS security settings. If this keeps happening, try contacting the website's owner.

Try this:

- Go back to the last page

Figure 6: Internet Explorer: Cannot securely connect to this page

In Firefox:



Secure Connection Failed

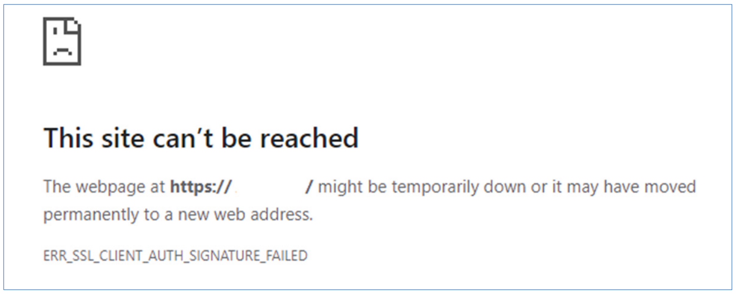
An error occurred during a connection to . A PKCS #11 module returned CKR_DEVICE_ERROR, indicating that a problem has occurred with the token or slot.

Error code: SEC_ERROR_PKCS11_DEVICE_ERROR

- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the website owners to inform them of this problem.

Figure 7: Firefox: Secure Connection Failed

In Chrome:



This site can’t be reached

The webpage at **https://** / might be temporarily down or it may have moved permanently to a new web address.

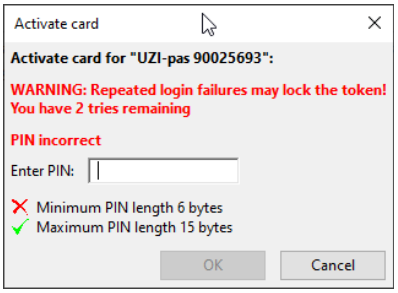
ERR_SSL_CLIENT_AUTH_SIGNATURE_FAILED

Figure 8: Chrome: This site can’t be reached

Note that the screenshots above are included as an example only. Actual error messages may differ.

3.2 Incorrect PIN during Activation UZI-pas 3

If the user enters an incorrect PIN when activating his UZI-pas 3 card, the following error message is displayed:



Activate card

Activate card for "UZI-pas 90025693":

WARNING: Repeated login failures may lock the token!
You have 2 tries remaining

PIN incorrect

Enter PIN:

✗ Minimum PIN length 6 bytes
✓ Maximum PIN length 15 bytes

Figure 9: Activate card: PIN incorrect

3.2.1 PIN Status and Retry Counter

A retry counter of three attempts exists for entering the correct PIN upon activation.

In the *Token Information* dialog (**Token > Show Token Info**), the status of the PIN is displayed.

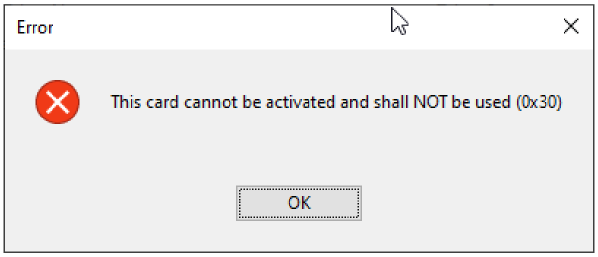
There are four possible scenarios:

1. OK
2. PIN has been entered incorrectly at least once
3. One final attempt left to enter the PIN correctly
4. LOCKED

In addition, when you perform an operation within the Token Administration Utility, such as Activate Card (or any other item for which PIN entry is required), you will also receive information on the status of the PIN in the dialog involved.

3.2.2 Locked PIN

If the user enters an incorrect PIN three times, the following error message will be displayed:



Error

This card cannot be activated and shall NOT be used (0x30)

Figure 10: Token Administration Utility: This card cannot be activated and shall NOT be used

The card cannot be activated and shall not be used.

The locked status of the PIN will be displayed in the *Token Information* dialog as well.

3.3 Change PIN of UZI-pas 3

It is possible to change the PIN for the UZI-pas 3 before the card is activated.

However, the user should nevertheless activate the card, before he is able to use it.

If he changes the PIN of the card before activating it, he should use this new PIN to activate the card.

3.4 Unblock the UZI-pas 3

If the user enters an incorrect PIN (three times) during activation of the UZI-pas 3 card, the PIN will be blocked.

However, if the user also knows the PUK, he will be unable to unlock the PIN with the PUK, upon which he can activate the card with the new PIN.