


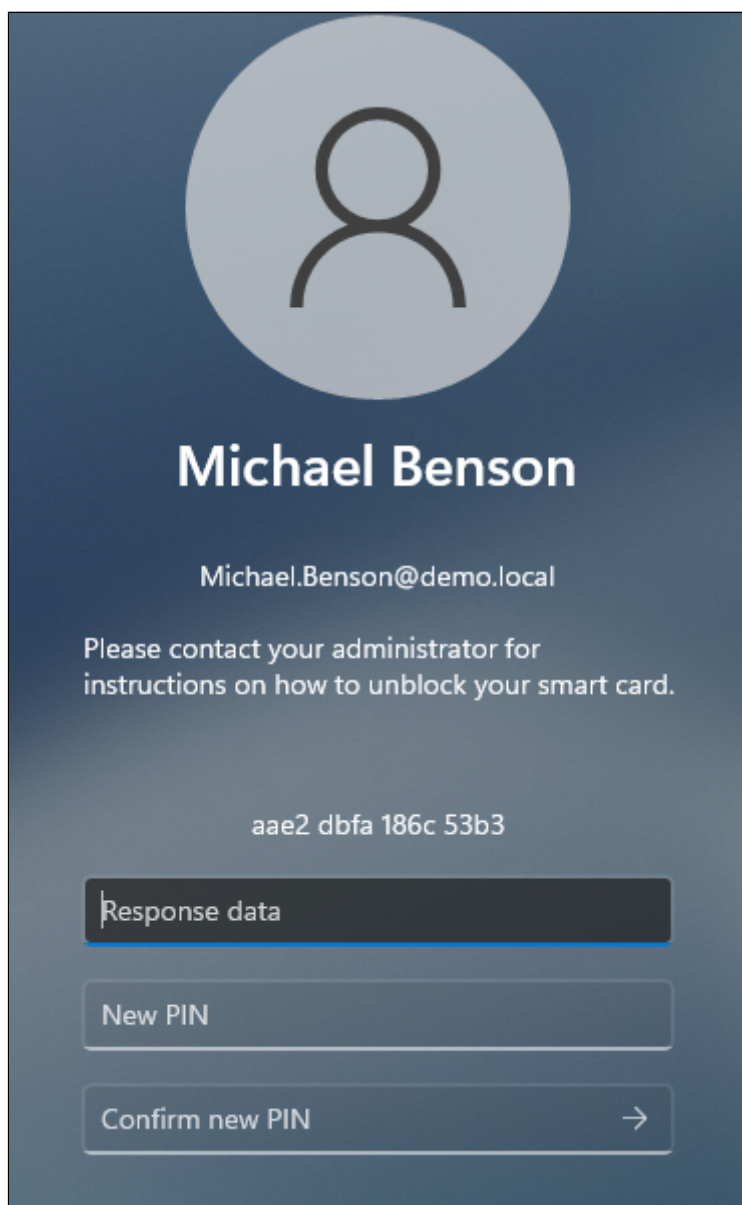
Offline unlocking on the Windows login screen

Offline unlocking is performed by system operator according to the principle of challenge-response authentication mechanism.

 Unlocking a card (Smart card, USB token) on the Windows login screen is not supported when connected remotely via Remote Desktop.


When the number of PIN input attempts is exceeded, the user receives a message that their card is locked. Along with that, the user receives a unique 16-character request code. The user has to communicate with the system administrator (by phone, for instance), authenticate their identity by answering the security questions and tell the received request code.

The figure shows an example of smart card offline unlocking window in Windows 11 interface.

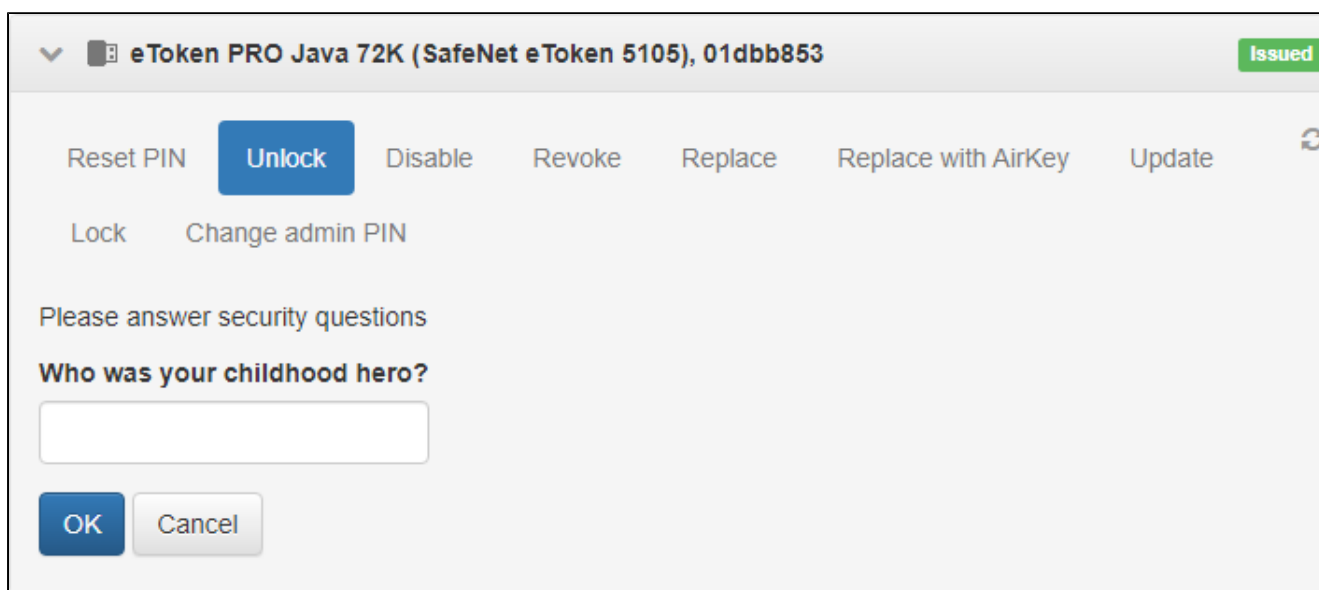



The image shows a Windows 11 smart card offline unlocking window. At the top, there is a large circular placeholder for a user profile picture. Below it, the name "Michael Benson" is displayed in a large, bold, white font. Underneath the name, the email address "Michael.Benson@demo.local" is shown in a smaller white font. A message in white text reads: "Please contact your administrator for instructions on how to unblock your smart card." Below this message, a 16-character request code "aae2 dbfa 186c 53b3" is displayed. There are three input fields at the bottom: the first is labeled "Response data" and has a blue border; the second is labeled "New PIN"; and the third is labeled "Confirm new PIN" and has a right-pointing arrow button next to it.

The system administrator opens the user card and selects **Unlock** item from the list of actions. Before generating the response code for card unlocking, the administrator has to ask security question (or several questions, depending on the policy settings) and enter the user response to the form.

 **Offline unlocking** can be disabled in the **Workflow** section of smart card usage policy. In this case the **Unlock** button is inactive in the user card.

The need to answer to security questions during offline unlocking is defined by **Validate answers to security questions** option.



▼  **eToken PRO Java 72K (SafeNet eToken 5105), 01dbb853** Issued

Reset PIN **Unlock** Disable Revoke Replace Replace with AirKey Update

Lock Change admin PIN


Please answer security questions

Who was your childhood hero?

OK Cancel

If the answers to all the questions are correct, the operator enters the code obtained from the user and the system generates the response code, which the operator tells to the user.

▼

 eToken PRO Java 72K (SafeNet eToken 5105), 01dbb853

Issued

Reset PIN

Unlock

Disable

Revoke

Replace

Replace with AirKey

Update

↺

Lock

Change admin PIN

Please enter challenge and click 'Get response'

Challenge

aae2 dbfa 186c 53b3


Response

207b 388a 1d88 b19d

Get response

Close

The user enters the response code and defines the new PIN for the smart card.



Michael Benson

Michael.Benson@demo.local

Please contact your administrator for instructions on how to unblock your smart card.

aae2 dbfa 186c 53b3

207b 388a 1d88 b19d

New PIN

Confirm new PIN →

If unlocking was successful, the corresponding message is displayed.



Michael Benson

The smart card has been unlocked successfully.

OK