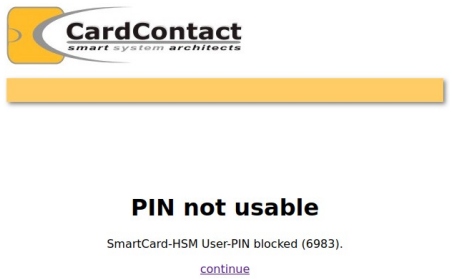
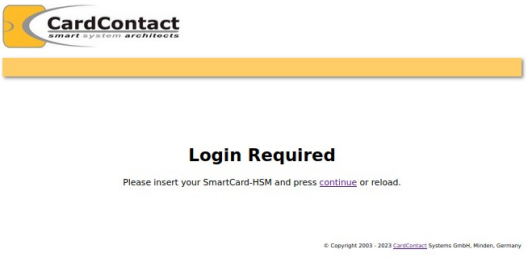
Einleitende Anmerkung zum Dokument für die Pin-Rücksetzung:
Das Dokument richtet sich gleichermaßen an Key-User bzw. Personen, die zur Pin-Rücksetzung berechtigt sind (im Folgenden unter KeyUser zusammengefasst), als auch an Smartcard-innehabende Personen, die eine Pinrücksetzung benötigen, als auch gegebenenfalls an Administratoren in den einzelnen Hochschulen .
Der der Prozess ein wechselseitiger ist und teilweise Interaktionen zwischen den Beteiligten erfordert, sind in diesem Dokument alle Schritte in zeitlicher Abfolge aufgeführt, die abwechselnd von den beteiligten Seiten durchgeführt werden müssen.
Zusätzlich sind noch einige Tätigkeiten erläutert, die als Voraussetzung für die Durchführbarkeit des Verfahrens notwendig sind, bei denen sowohl die Zuständigkeit (KeyUser, Administrator, die Nutzenden selber) als auch die Art der Durchführung sich in den einzelnen Hochschulen unterscheiden können, wie zum Beispiel der Start der ocf-cc.jar-Datei für die Anmeldung an smartcard.ccc.uni-hannover.de oder der Start der ocf-cc.jar-Datei zur Verbindung der Smartcard zum Management-Token für die Pin-Rücksetzung.
Bei den einzelnen Schritten ist jeweils vermerkt, an wen sich diese Erläuterung wahrscheinlich richtet, das kann jedoch in jeder Hochschule leicht abweichen. Aus diesem Grund ist auch des komplette Verfahren in einem Dokument zusammengefasst, unabhängig davon, welche Person nun die welchen Schritt durchführt. So haben auch alle am Prozess Beteiligten einen Überblick, welche Tätigkeiten zu dem Prozess gehören und wie der Ablauf der einzelnen Schritte erfolgen muss.

Die Prozessbeschreibung beginnt hier - mit der Vorstellung einer Blockierten Smartcard:

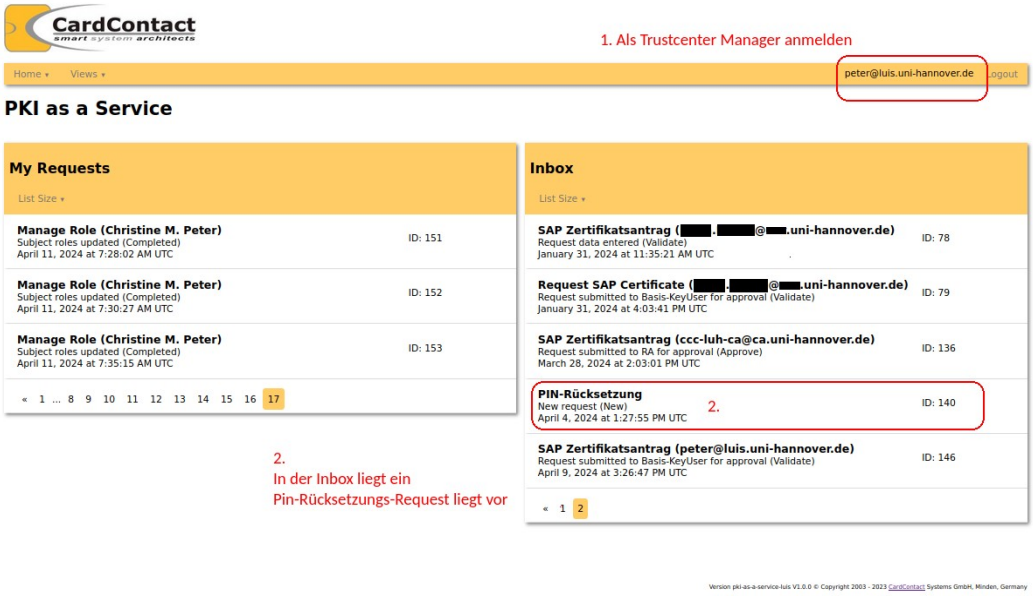


Betrifft Nutzende mit blockierter Smartcard
Nutzende sehen die Meldung, dass die Pin blockiert ist. Kontaktaufnahme zum SAP-KeyUser erforderlich. Hochschulintern muss geregelt werden, ob persönliches Erscheinen notwendig ist oder – falls nicht – wie die Identität der Person mit einer Pin-Rücksetzungs-Anforderung durch organisatorische Maßnahmen überprüft und bestätigt wird.

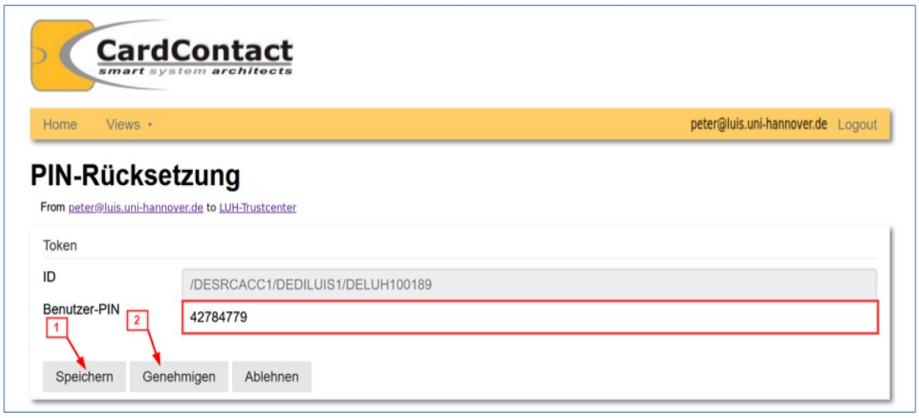


Betrifft die zur Entsperrung berechtigte Person
(in der Regel Keyuser mit der Rolle Trustcenter Manager)

Trustcenter Manager meldet sich an smartcard.ccc.uni-hannover.de an.
„continue“ klicken



Betrifft die zur Entsperrung berechtigte Person



Betrifft die zur Entsperrung berechtigte Person

Hier die PIN auf eine 8-stellige Zahl erweitern, Speichern und Genehmigen.

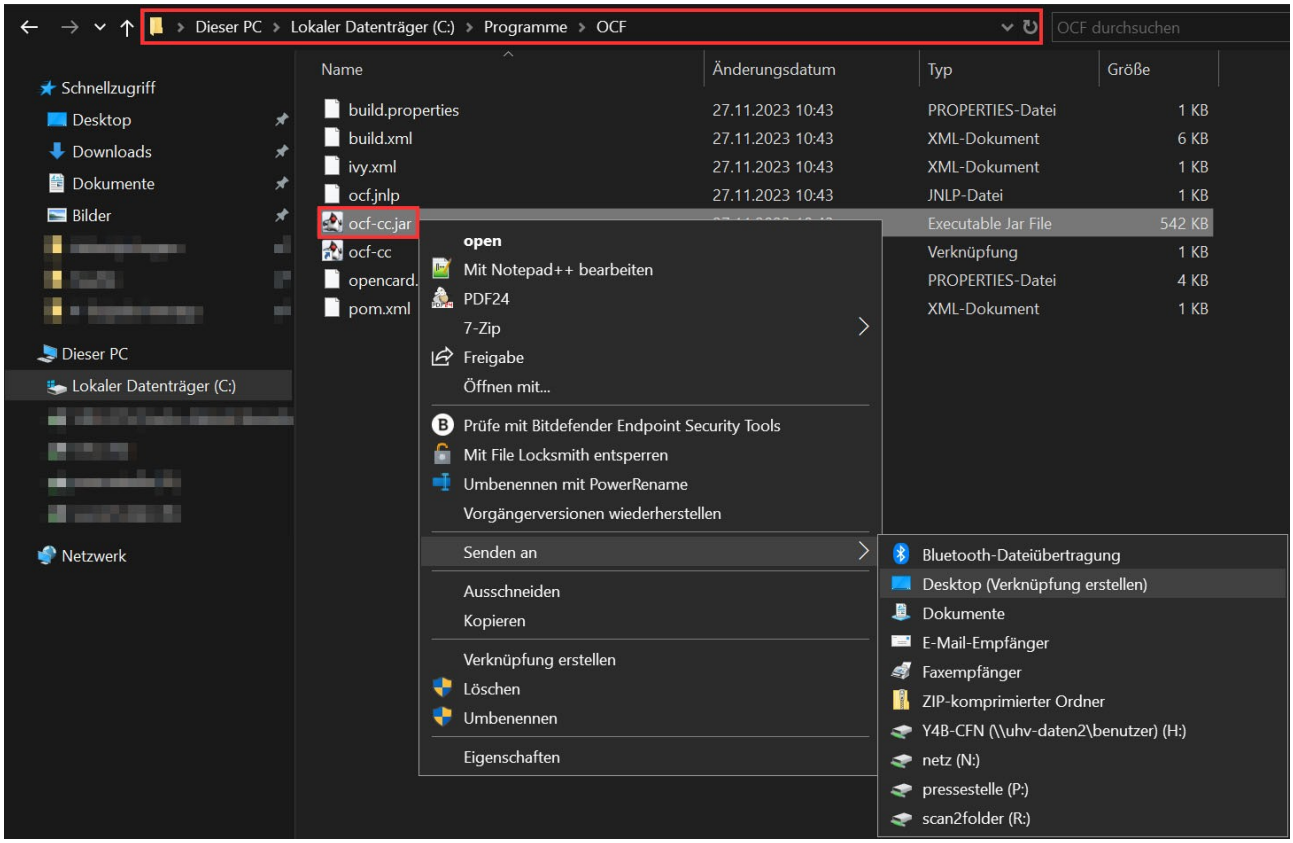
Richtet Sich an KeyUser oder Administratoren oder in Teilen auch an die Nutzenden selbst:

Für die Entsperrung der Karte muss sich die Smartcard mittels Aufruf von
ocf-cc.jar mit dem Parameter https://luis.pki-as-a-service.net/rt/paas
noch mit dem Management-Token des Trustcenters verbinden um die neue Pin noch auf die Smartcard zu übertragen.

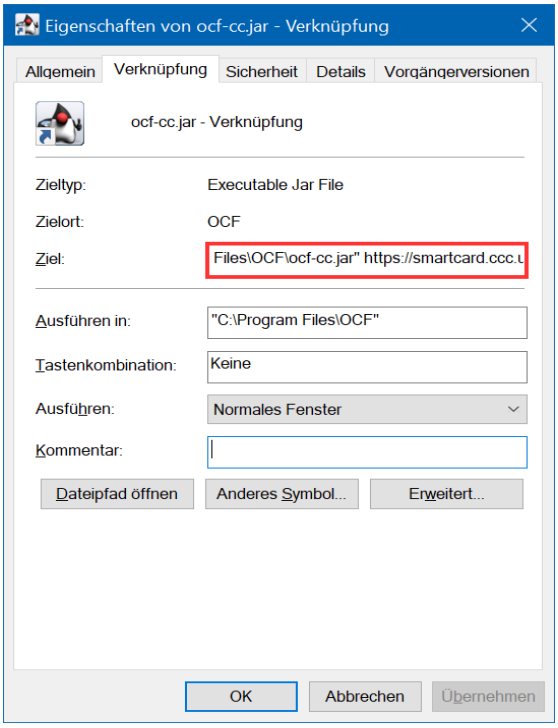
Dazu sollte auf dem Desktop der Personen die mit Smartcards arbeiten, eine entsprechende Verknüpfung für den Aufruf von java -jar ocf_cc.jar https://luis.pki-as-a-service.net/rt/paas zur Verfügung stehen.

Möglichkeit 1, eine Verknüpfung der Datei ocf-cc.jar auf dem Desktop anzulegen:
Über das Anlegen einer Textdatei die den Befehl:
java -jar ocf_cc.jar https://luis.pki-as-a-service.net/rt/paas
enthält, ergänzt um die Verzeichnisse, im denen Java und/oder ocf_cc.jar liegen oder anpassen der Path-Variable.
Diese Datei kann unter unter einem beliebigen Namen, z.b. Kartenupdate.cmd abgespeichert werden und als Verknüpfung auf dem Desktop zur Verfügung gestellt werden.

Möglichkeit 2, eine Verknüpfung der Datei ocf-cc.jar auf dem Desktop anzulegen:



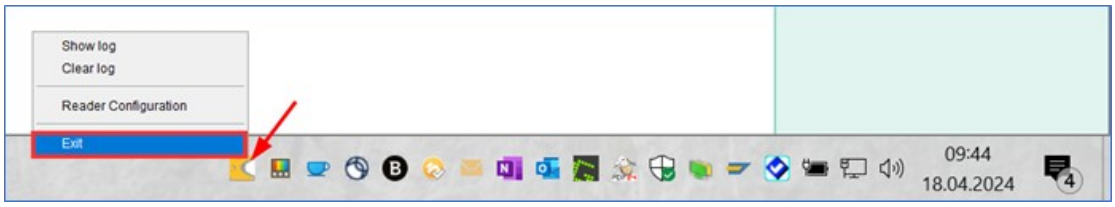
Gehen Sie über Ihren Dateimanager in das Verzeichnis, in dem die Datei ocf-cc.jar gespeichert ist:
Erzeugen Sie wie in dem Screenshot oben dargestellt eine Verknüpfung auf dem Desktop.



Bei der Verknüpfung muss unter „Eigenschaften“ im Feld „Ziel“ noch https://smartcard.ccc.uni-hannover.de/rt/paas ergänzt werden, getrennt durch ein Leerzeichen.

Ab hier kann die weitere Bearbeitung auch am Arbeitsplatz der karteninhabenden Person durch diese selbst erfolgen.

Dazu müssen folgende Schritte durchgeführt werden:
Die Datei ocf-cc.jar (auch Card Updater Daemon) muss beendet werden, wenn sie gestartet ist. Man erkennt das an einem gelben Icon mit weißem Halbkreis im System-Tray (s. Screenshot).



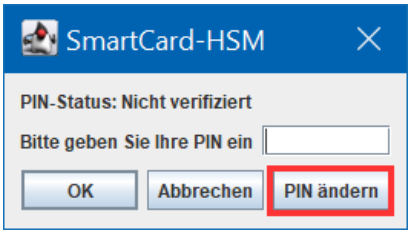
Mit der rechten Maustaste auf das Icon klicken und „Exit“ auswählen.

Die Datei ocf-cc.jar muss nun erneut gestartet werden, aber mit einem Parameter, der dafür sorgt, dass die Karte sich mit dem Management-Token verbindet.

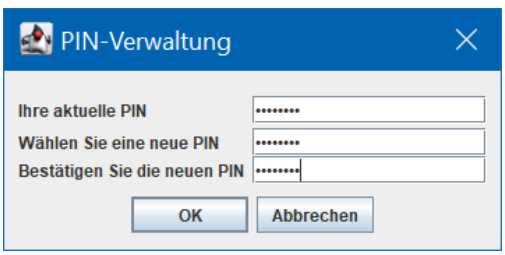
Dazu sollten Sie auf Ihrem Desktop eine Datei zur Verfügung gestellt bekommen haben, und von Ihrem Ansprechpartner (Administrator und/oder SAP-KeyUser die entsprechende Information erhalten haben. Die Verknüpfung könnte „ Kartenupdate.cmd“ heissen oder eine Verknüpfung auf dem Desktop namens „ocf-cc.jar“ und dem Ziel „https://luis.pki-as-a-service.net/rt/paas“ (sichtbar in den Eigenschaften der Verknüpfung).
Sie können auch durch Ausführung der oben erläuterten Schritte zum Anlegen der Verknüpfung (**Möglichkeit 1** oder **Möglichkeit 2**) selber versuchen, sich die Verknüpfung zu erstellen. Sollten Sie jedoch allein nicht weiterkommen, und keine Informationen haben, nehmen Sie Kontakt zu Ihrem Administrator oder zum KeyUser Ihrer Hochschule auf.

Haben Sie diese Verknüpfung zur Verfügung, können Sie fortfahren:
Die Karte muss in das Lesegerät gesteckt und die Verknüpfung gestartet werden.
Es geht kein Programmfenster auf, es erfolgt nur ein Zugriff auf Ihre Smartcard, das Lesegerät blinkt kurz.
Nun muss wieder die Datei ocf-cc.jar gestartet werden und zwar auf dem „normal üblichen Weg“ ohne den extra-Parameter zur den Zugriff auf das Management Token.

Anschließend im Web-Browser auf https://smartcard.ccc.uni-hannover.de anmelden. Wenn alles geklappt hat, erscheint das Anmeldefenster für Ihre Smartcard:



Bitte dann als erstes Ihre Pin ändern.
Die Pin die aktuell vergeben ist, und die Sie im Verlauf des Rücksetzungsprozesses erhalten haben, ist je mehr Personen als Ihnen bekannt. Also „PIN ändern“ anklicken.



Bitte geben Sie unter „aktuelle PIN! Ihre nach der Rücksetzung übermittelte PIN ein. Vergeben Sie sich dann unter „Wählen Sie eine neue PIN“ eine eigene PIN und bestätigen Sie diese durch „OK“.
Der Vorgang der Pin-Rücksetzung ist nun abgeschlossen.