Bedienungsanleitung PersonalausweisCredentialProvider

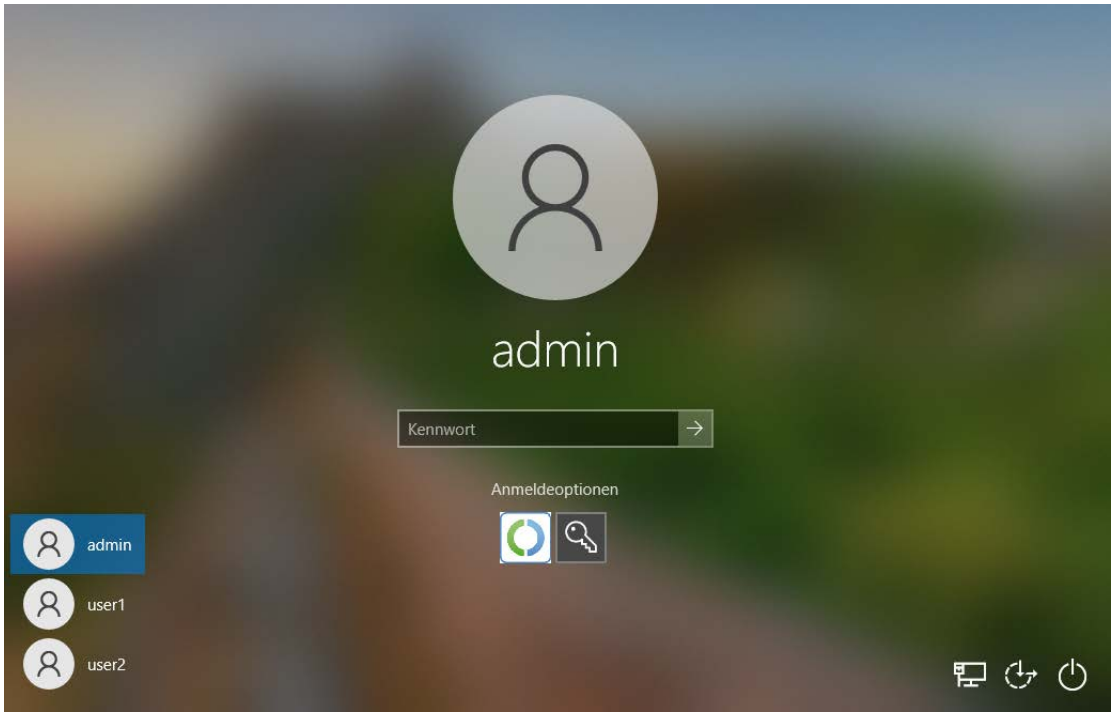
Stand 07.07.2021

PersonalausweisCredentialProvider ist ein neuer V2 Custom credential provider für Windows 10 von buergerservice.org e.V.

Microsoft:
https://docs.microsoft.com/en-us/windows/win32/secauthn/credential-providers-in-windows#custom-credential-providers

Der Credential Provider ermöglicht eine Zwei-Faktor-Authentisierung, dh zusätzlich zu dem Faktor Wissen wie Passwort/PIN kommt der Faktor Besitz, in diesem Fall der Besitz des Personalausweises. Dadurch wird die Winlogon-Sicherheit erhöht.

Voraussetzungen:
ein 64bit Computer (weil PersonalausweisCredentialProvider 64bit ist),
Windows 10
Visual C++ Redistributable for Visual Studio 2015/2017/2019
AusweisApp2 installiert für alle Benutzer,
Kartenleser,
Personalausweis (ob dieser auslesbar ist kann in AusweisApp2 unter "Meine Daten einsehen" getestet werden)
Internetanschluss



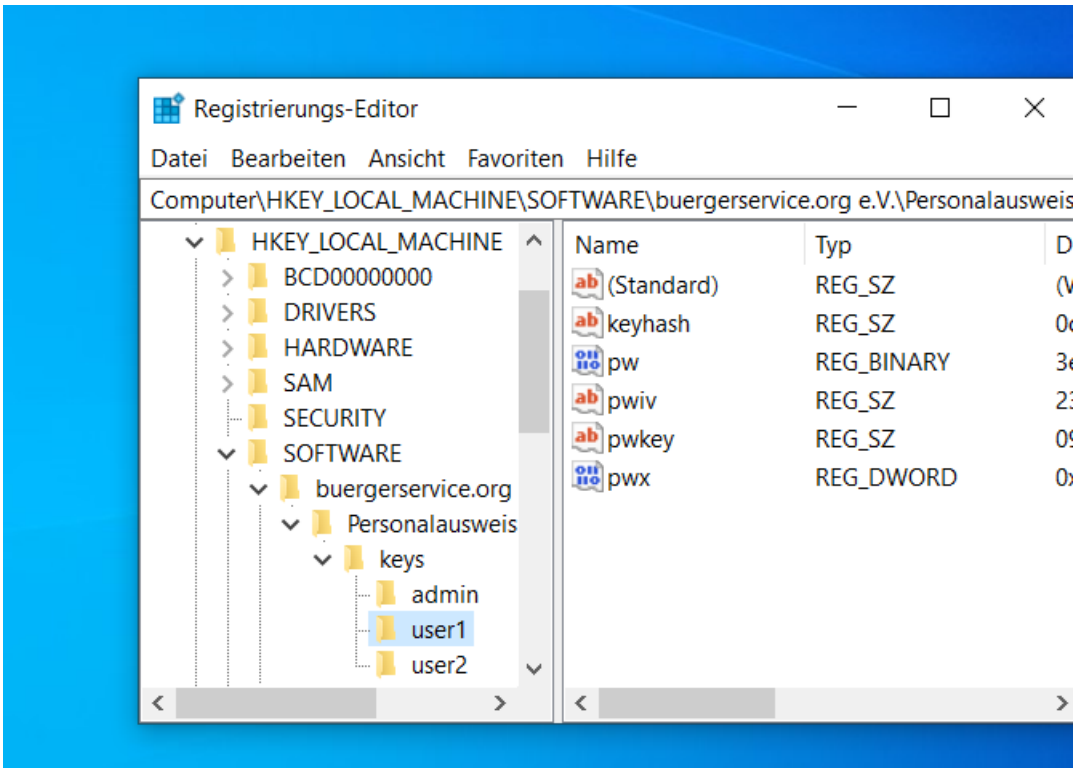
Installation:

Bevor Sie beginnen stellen Sie als Admin sicher dass Sie von allen Benutzern die hashkeys vorliegen haben Der hashkey kann mit workflowClient.exe <PIN> angezeigt werden (am Ende der Ausgabe). Also die Zeichen in der Zeile unter “keyhash of workflow:” ohne Leerzeichen.
Eine andere Möglichkeit ist im Personalausweis Credential Provider mit der Option “Zeige Personalausweisschlüssel” sich den Hashkey anzeigen zu lassen wenn zB ein neuer User dazukommt. Das wird unter dem betreffenden Punkt später genauer beschrieben.

Als Admin kopieren Sie PersonalausweisV2CredentialProvider.dll unter windows/system32

Registrieren Sie die dll mit register_PersonalausweisV2CredentialProvider.reg

Bevor Sie neu starten legen Sie für alle lokalen Benutzer als Admin cmd das setuserregistry.exe
setuserregistry.exe user hashkey <optionalesPasswort>
Wenn Sie kein optionales Passwort angeben wird eines generiert.
Hashkey des users und das Passwort werden in der registry unter Computer\HKEY_LOCAL_MACHINE\SOFTWARE\buergerservice.org e.V.\PersonalausweisCredentialProvider\keys in directories pro user angelegt. Falls der Admin ein Sicherheitsproblem damit sieht dass alle user dort einsehen können, kann er die Berechtigungen der user-diretories so ändern dass nur der betreffende Benutzer einsehen kann statt alle Benutzer (+system+admin usw natürlich).



Mit regedit können Sie hinterher kontrollieren ob wirklich für jeden user dort ein directory vorhanden ist in dem jeweils 5 Werte angelegt sein müssen.

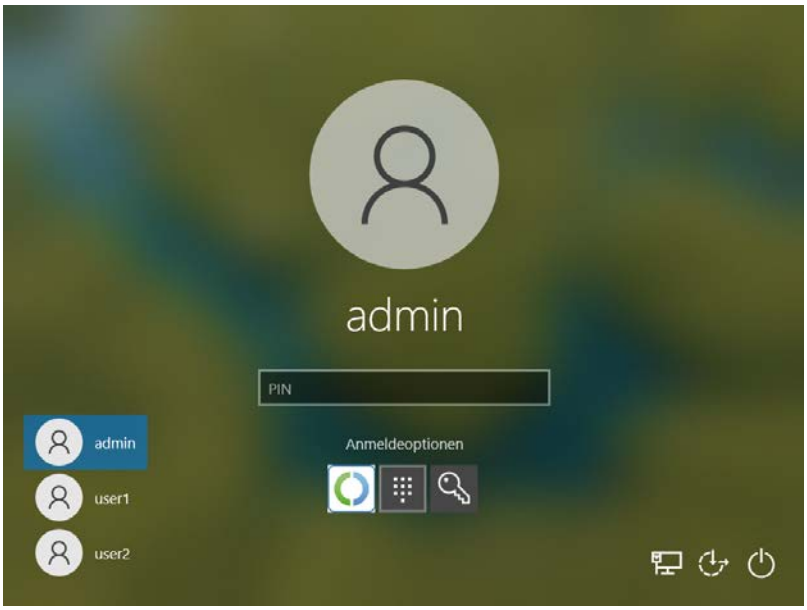
Starten Sie den Batch makelinkProgramme.bat
Dieser sollte links von Programme zu Programs anlegen. Wenn Sie in cmd unter c:\ den Befehl dir eingeben sollten die links als <JUNCTION> angezeigt werden.

Prüfen Sie noch einmal die Voraussetzungen (siehe oben) ob alles vorhanden ist.

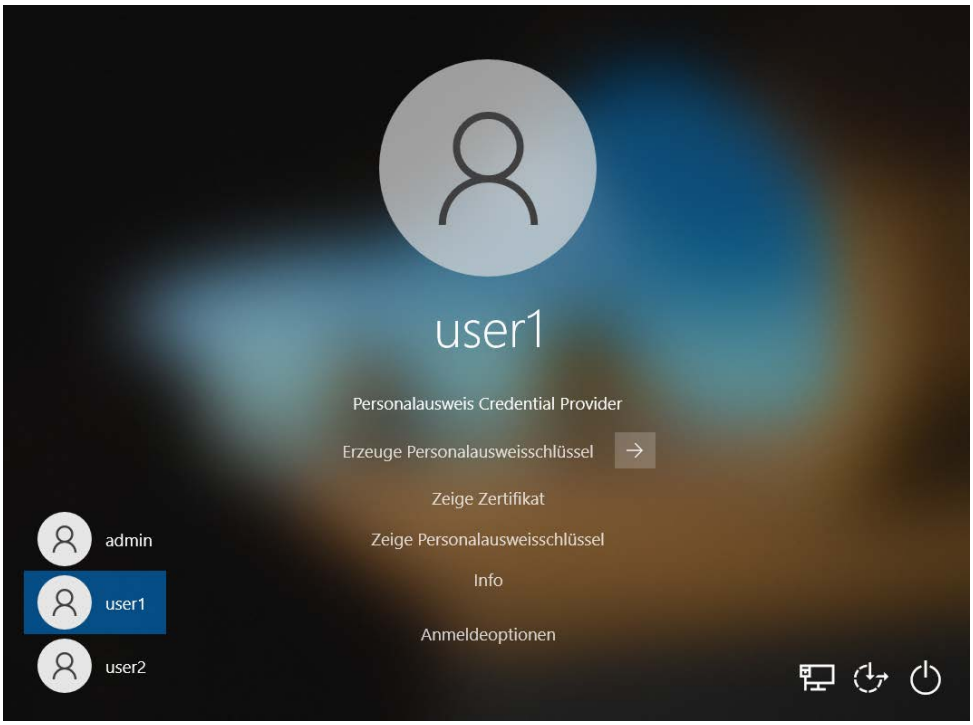
Benutzung:

Nach einem Neustart sollte der PersonalausweisCredentialProvider sichtbar sein.

Falls Sie alle anderen CredentialProvider nicht deaktiviert haben ist er in der Liste der Provider angezeigt (hier der links unter Anmeldeoptionen):

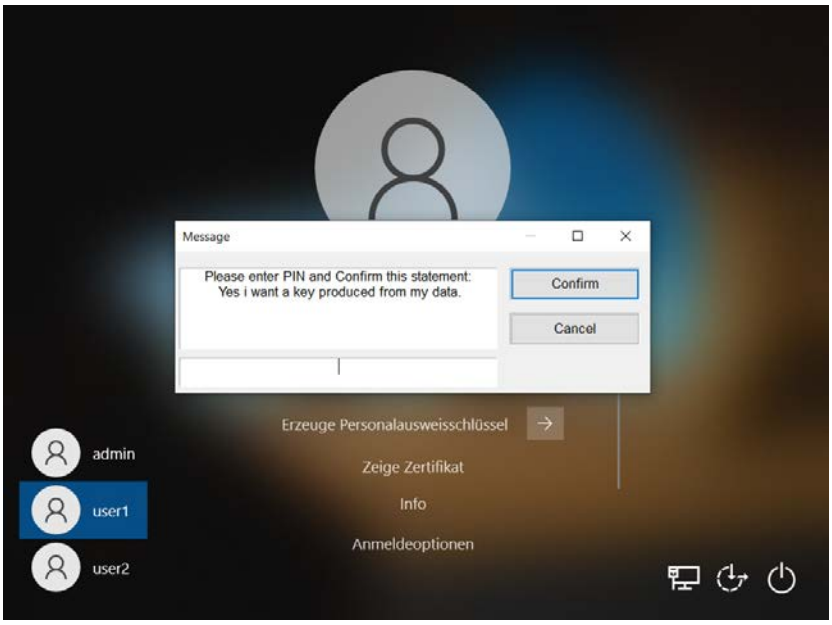


Mit einem Klick auf das Logo kommen Sie in den PersonalausweisCredentialProvider.
Es gibt die Möglichkeit einen Personalausweisschlüssel zu erzeugen, das Zertifikat, den Personalausweisschlüssel und Infos anzeigen zu lassen.

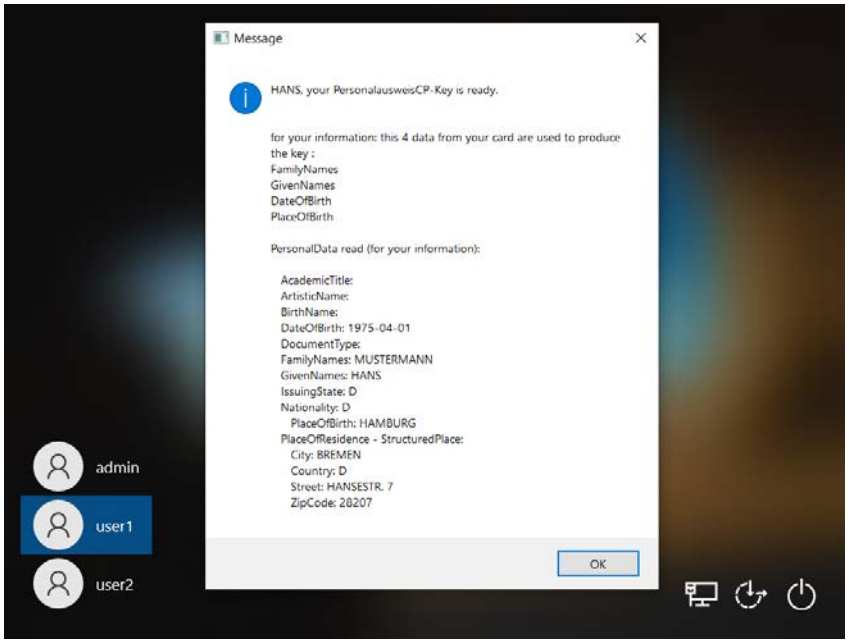


Einloggen:

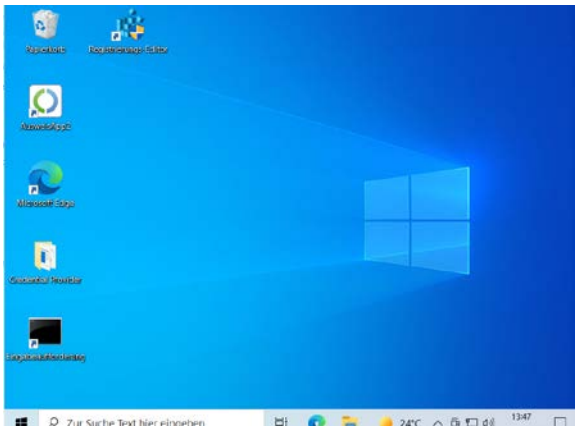
Legen Sie den Personalausweis auf/in ihren Kartenleser. Erstellen Sie einen Personalausweisschlüssel durch Anwählen von “Erzeuge Personalausweisschlüssel”. Falls ihr Kartenleser kein keypad besitzt wird die PIN des Ausweises abgefragt ansonsten müssen Sie die PIN am keypad eingeben:



Wenn die Selbstauskunft startet kommt ein kleines Fenster “selfauthentication is running.”. Dieses Fenster schliesst sich selbstständig wenn die Selbstauskunft fertig ist.

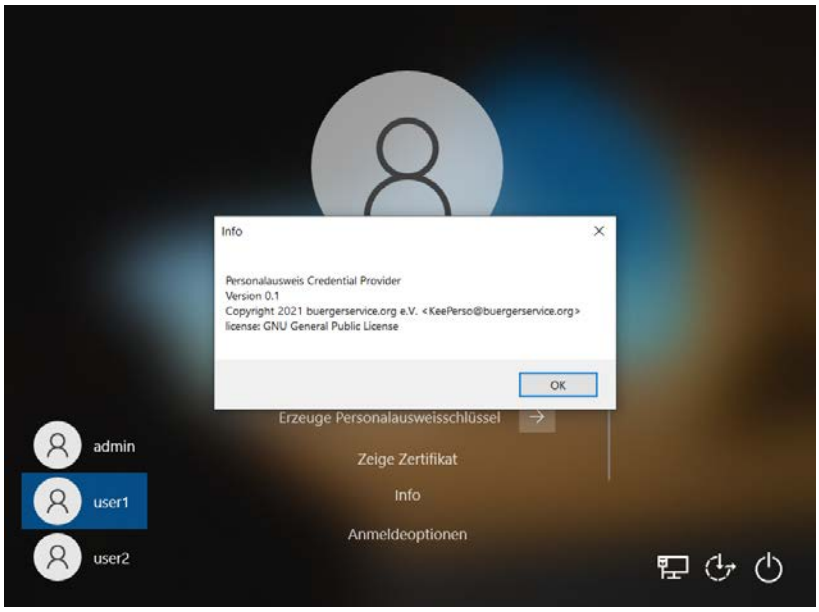


Wenn Sie auf den Übermitteln-Button klicken (Pfeil nach rechts) wird der Personalausweisschlüssel (=hashkey des users) mit dem entsprechenden Schlüssel in der registry verglichen. Sind sie gleich wird der Benutzer in Windows eingeloggt. Der Benutzer hat sich erfolgreich eingeloggt.

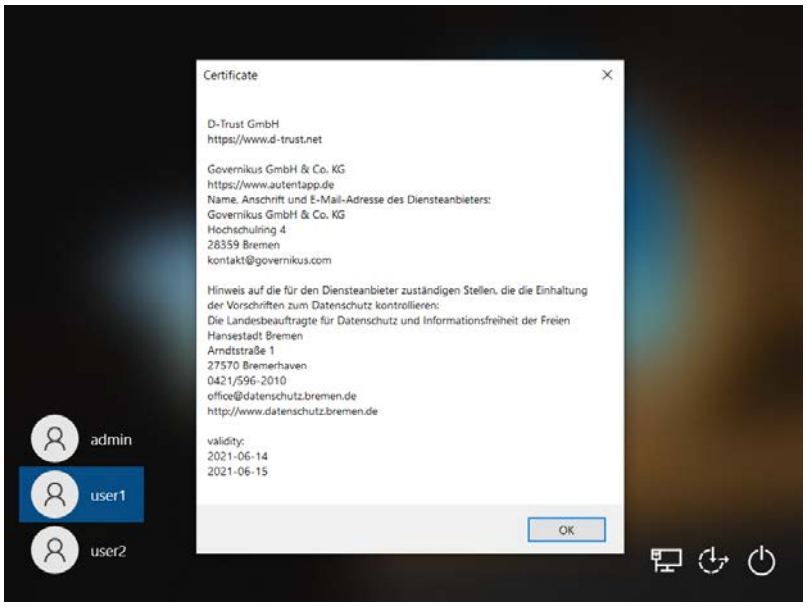


Weitere Optionen im PersonalausweisCredentialProvider

Info:

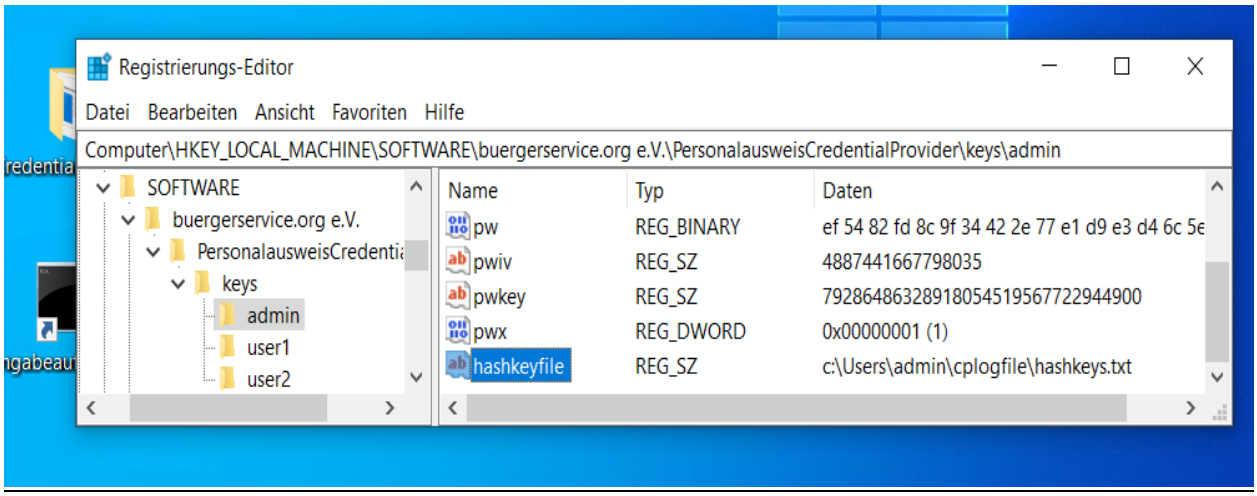


Zertifikat:



Zeige Personalausweisschlüssel:

Hier kann man sich den Personalausweisschlüssel anzeigen lassen. Es ist möglich dass zB sich der Admin hier auch von einem neuen Benutzer den Schlüssel anzeigen lassen kann um ihn später mit setuserregisty.exe administrieren zu können. Wenn der Admin unter Computer\HKEY_LOCAL_MACHINE\SOFTWARE\buergerservice.org e.V.\PersonalausweisCredentialProvider\keys zb in seinem directory zB admin einen String-Wert mit Namen hashkeyfile anlegt und dort hinterlegt wo die hashkeys als Textdatei abgelegt werden sollen. Das Verzeichnis für die Textdatei muss vorhanden sein, die Datei wird erzeugt falls sie nicht vorhanden ist. Die hashkeys werden mit Zeitstempel abgespeichert.



Abschalten von Providern:

Unter Methode 2 wird hier von Microsoft beschrieben, wie man nicht benötigte/erwünschte Provider abschalten kann, zb den Kennwortprovider (im abgesicherten Modus steht er dem Admin trotzdem zur Verfügung). Man muss in dem Provider ein DWORD **“Disabled”** mit Wert 1 anlegen.

https://social.technet.microsoft.com/Forums/windows/de-DE/9c23976a-3e2b-4b71-9f19-83ee3df0848b/how-to-disable-additional-credential-providers?forum=w8itprosecurity

Probleme:

Sollten Probleme auftreten kann der Admin sich in den abgesicherten Modus mit seinem Kennwort einloggen. Dann kann der in windows/system32 die Datei PersonalausweisV2CredentialProvider.dll löschen. Durch den Start von Unregister_PersonalausweisV2CredentialProvider.reg wird der PersonalausweisCredentialProvider deregistriert.