Implementation flaw in Windows Hello biometrics

© 2022 Passcape Software
Passcape Software

1. Implementation flaw in Windows Hello biometrics 3
1.1 Brief overview 3
1.2 OSes affected 3
1.3 What is Windows Hello biometrics? 3
1.4 What is DPAPI? 3
1.5 Description of the mis-implementation in Windows Hello biometric authentication 4
1.6 What data is at risk? 4
1.7 PoC 4
1.8 Conclusion 8

© 2022 Passcape Software

1 Implementation flaw in Windows Hello biometrics

1.1 Brief overview

Using Windows Hello biometric authentication compromises all personal data encrypted with DPAPI.

1.2 OSes affected

If the TPM protection is not set, all versions of Windows 10 and 11 are affected, all local accounts, as well as Microsoft and Azure AD ones.

1.3 What is Windows Hello biometrics?

Unlike a common password authentication, Windows Hello biometrics is a new, easy and supposedly safer way to sign into Windows using your unique physical characteristics. The Windows Hello biometrics was first introduced in Windows 10 and included fingerprint and face recognition technology.

The Windows Hello allows users to securely log into devices that have the necessary hardware components without having to type a password. You will have to work hard to forget or alter your biometric data, because it's an integral part of your personal identity. Moreover, the biometric authentication, either a facial recognition or a fingerprint scanning, is more convenient and faster compared to the process of typing a password.

1.4 What is DPAPI?

Data **P**rotection **A**pplication **P**rogramming **I**nterface is a primary data protection subsystem in all Windows Operating Systems since Win2K. DPAPI is used both by applications to protect their private information against the prying eyes and by the system to keep your personal data safe and secure. Such as network passwords, digital certificates and private encryption keys, authentication tokens, etc. If you want to deep down into the way the DPAPI works, its algorithms and principles, welcome to our blog.

© 2022 Passcape Software

1.5 Description of the mis-implementation in Windows Hello biometric authentication

Windows 10 - 11 DPAPI implementation is fully compatible with Windows Hello biometric authentication. So it's possible, besides using your logon password, to decrypt any DPAPI-protected data directly with a fingerprint or a facial recognition. The problem is that neither a fingerprinting nor a facial recognition is required to do that, since the user profile directly stores everything necessary for the successful decryption. Assuming that the appropriate authentication method has been already configured for the user account previously.

1.6 What data is at risk?

All DPAPI-protected data is at risk as soon as all of the following conditions are met:

- The source operating system is Microsoft Windows 10 or higher;
- The user account type is local, Microsoft, or Azure AD;
- The user account is configured to log in using Windows Hello biometrics;
- The TPM protection is off;

Some examples of the personal data protected with DPAPI

- Passwords to Web-sites, cookies and credit cards stored by popular browsers: Google Chrome, Microsoft Edge, Opera browser, etc.
- Passwords for some popular e-mail clients. Such as Microsoft Office Outlook, Windows Mail. Encryption keys for S-MIME.
- Credentials to shared resources.
- Encryption keys and passwords stored in Windows Vault.
- Remote Desktop credentials.
- EFS encryption keys.
- Users' personal certificates.
- Network credentials stored in Credential Manager. Including authentication tokens and other private information.
- Personal data in any application that uses DPAPI, such as Skype, Windows Rights Management Services, Windows Media and so on.

1.7 PoC

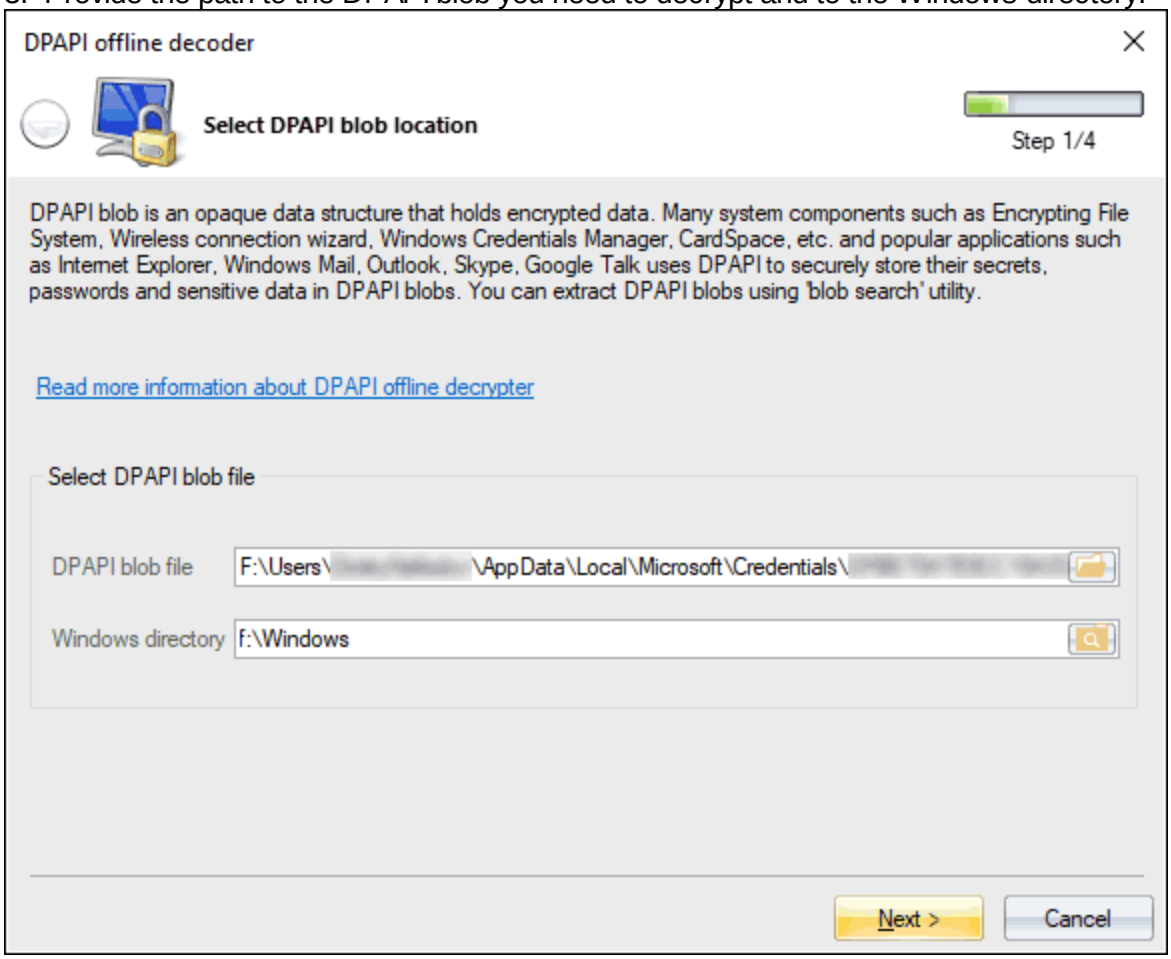
Here's a step-by-step instruction on how to decrypt a DPAPI blob without knowing the user logon password.

© 2022 Passcape Software

1. Attach the external disk drive that contain a biometric account to your PC. In the case of a virtual disk, make sure it has read-write permissions. Otherwise, the program will not be able to get access to the Windows Hello protected folders. On the screenshots below, the system assigned letter F: for the externally connected drive.

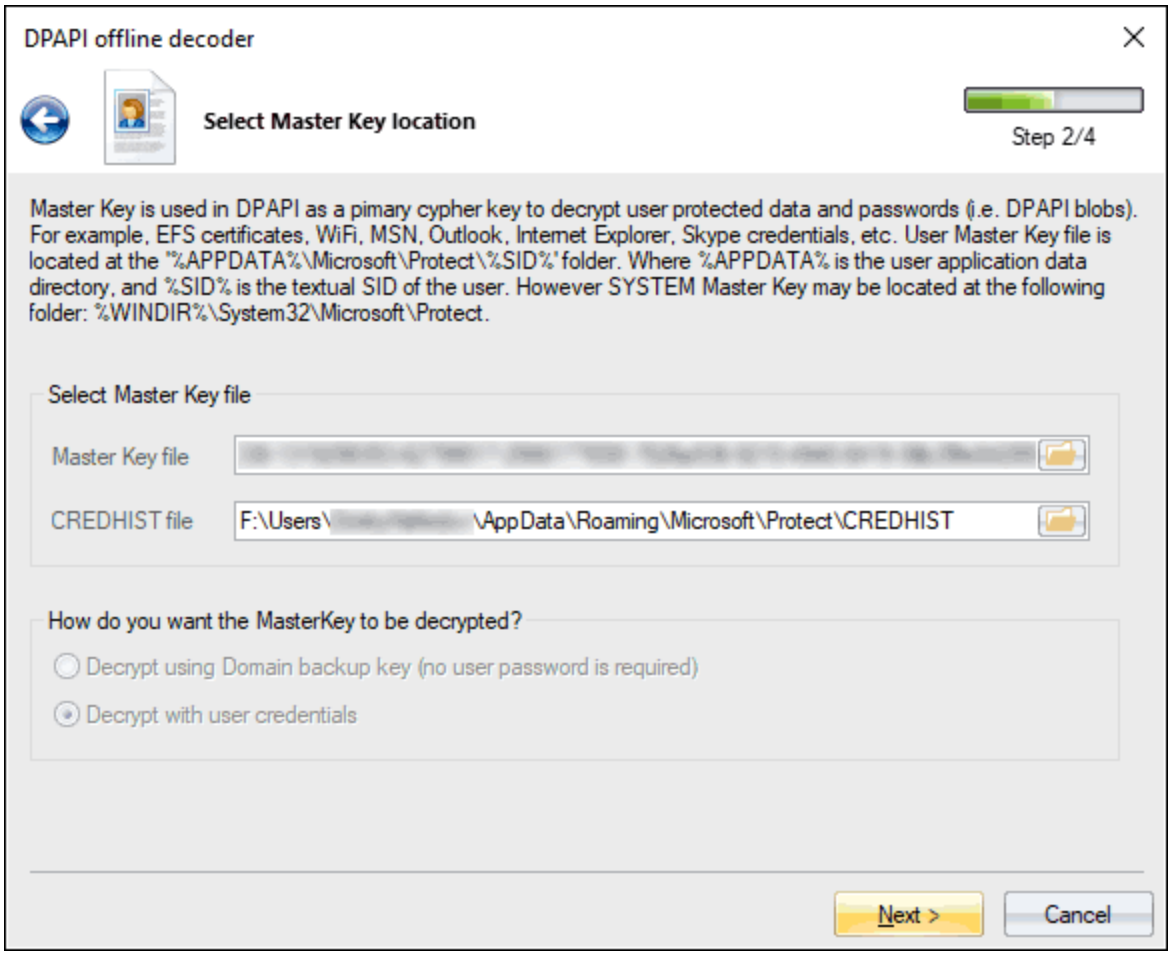
2. Run the Windows Password Recovery, locate the menu 'Utils', and then 'DPAPI decoder and analyzer -> Decrypt DPAPI data blob'

3. Provide the path to the DPAPI blob you need to decrypt and to the Windows directory.



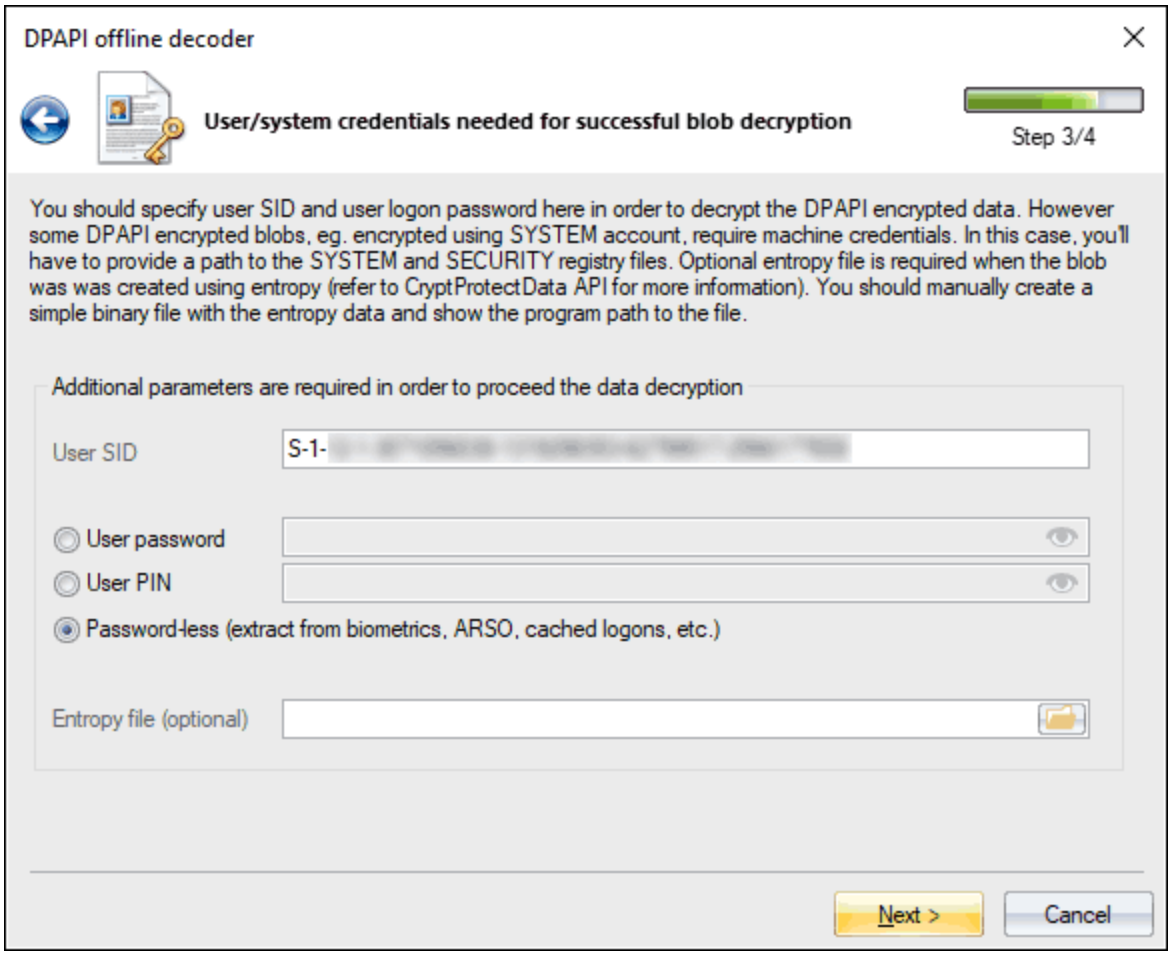
4. In the next dialog, specify the path to the master key. All user's master keys live in **%USER_PROFILE%\AppData\Roaming\Microsoft\Protect** folder.

© 2022 Passcape Software

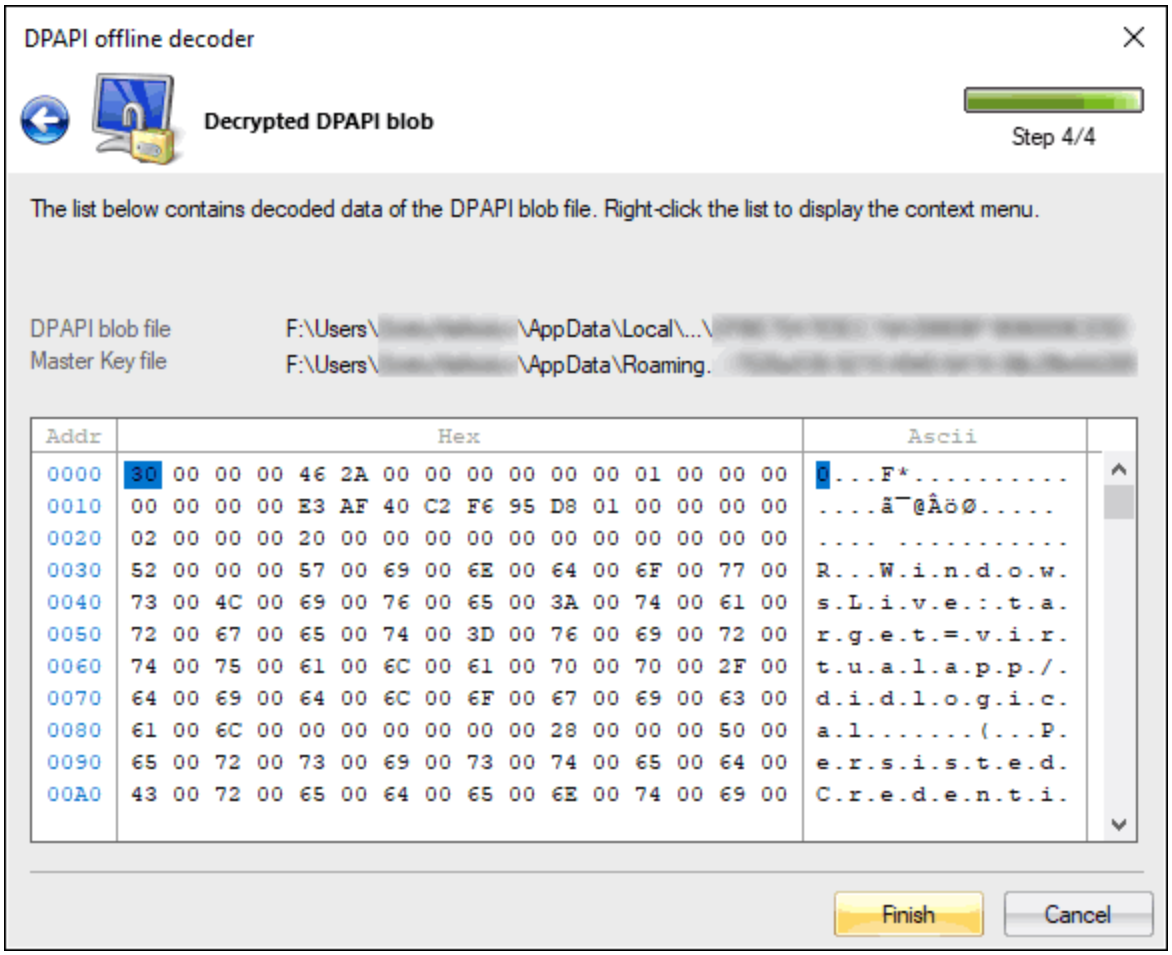


5. Now select the '*Password-less*' and click the '*Next*' button to finalize the decryption.

© 2022 Passcape Software



© 2022 Passcape Software



1.8 Conclusion

Despite all Microsoft's assurances about the safety of the biometric authentication, we see that this is not quite true, to put it mildly.

If your account uses a biometric authentication with the TPM protection set off, be extremely careful. All your personal data is at potential risk!

To protect your personal information, consider setting on a full disk encryption, turning the TPM protection on (of course, if your hardware supports it) or stop using the biometric authentication at all.

© 2022 Passcape Software