Уязвимость учетных записей с биометрической аутентификацией в Windows 10-11

Passcape Software

1 Уязвимость биометрической аутентификации Windows

1.1 Краткое описание

Использование биометрической аутентификации Windows Hello ставит под угрозу персональные данные, защищенные при помощи DPAPI.

1.2 Какие ОС затрагивает

Уязвимости подвержены все версии Windows 10 и Windows 11, все локальные учетные записи, а также учетные записи Microsoft и Azure AD, с отключенной опцией TPM.

1.3 Что такое биометрия Windows Hello

В отличие от обычной аутентификации по паролю, операционные системы Windows 10 и 11 предлагают новый, более простой и, предположительно, более безопасный способ входа в систему при помощи физических характеристик, уникальных для каждого человека. Таких как отпечатки пальцев или слепок лица.

Забыть свои биометрические данные довольно сложно, т.к. они всегда при вас. Кроме того, при биометрическом входе в систему сканирование лица или пальцев происходит быстрее, чем пользователь вводит пароль.

1.4 Что такое DPAPI

Data Protection Application Programming Interface или сокращенно DPAPI - является основным механизмом защиты персональных данных пользователя во всех операционных системах Windows, начиная с Windows 2000. DPAPI используется везде, где необходимо обеспечить сохранность и безопасность персональных данных. Таких как сетевые пароли, цифровые сертификаты и приватные ключи шифрования, токены аутентификации и т.д. Подробнее об устройстве и принципах работы DPAPI можно почитать в нашем блоге.

1.5 Описание уязвимости

В операционных системах Windows 10 и выше DPAPI полностью совместима с биометрической аутентификацией Windows Hello. Таким образом, персональные данные, защищенные DPAPI, можно расшифровать при помощи как отпечатка пальца, так и виртуального слепка лица (если были настроены соответствующие методы аутентификации). Проблема в том, что для этого непосредственно не требуется ни сам палец, ни лицо пользователя т.к. все необходимое для расшифровки хранится непосредственно на компьютере.

1.6 Какие данные в опасности

В опасности все данные DPAPI при соблюдении следующих условий:
- Операционная система Windows 10 или Windows 11
- Локальная учетная запись, учетная запись Microsoft или Azure AD
- В учетной записи настроен вход в систему при помощи биометрии Windows Hello
- Отключена опция TPM

Примеры персональных данных, зашифрованных DPAPI

- Пароли Веб сайтов, которые хранятся в популярных интернет обозревателях: Google Chrome, Microsoft Edge, Opera browser и др. Сохраненные кукисы и данные кредитных карт.
- Пароли почтовых клиентов Microsoft Office Outlook, Windows Mail. Ключи шифрования почты S-MIME.
- Пароли доступа к общим папкам и ресурсам
- Пароли и ключи шифрования, хранимые в Windows Vault
- Пароли соединений удаленного доступа к рабочему столу
- Ключи шифрования EFS
- Сертификаты пользователя
- Сетевые пароли, хранимые в Credential Manager. Включая токены аутентификации.
- Персональные данные любого приложения, защищенные при помощи DPAPI. Такие как Skype, Windows Rights Management Services, Windows Media, Google Talk и другие.

1.7 PoC

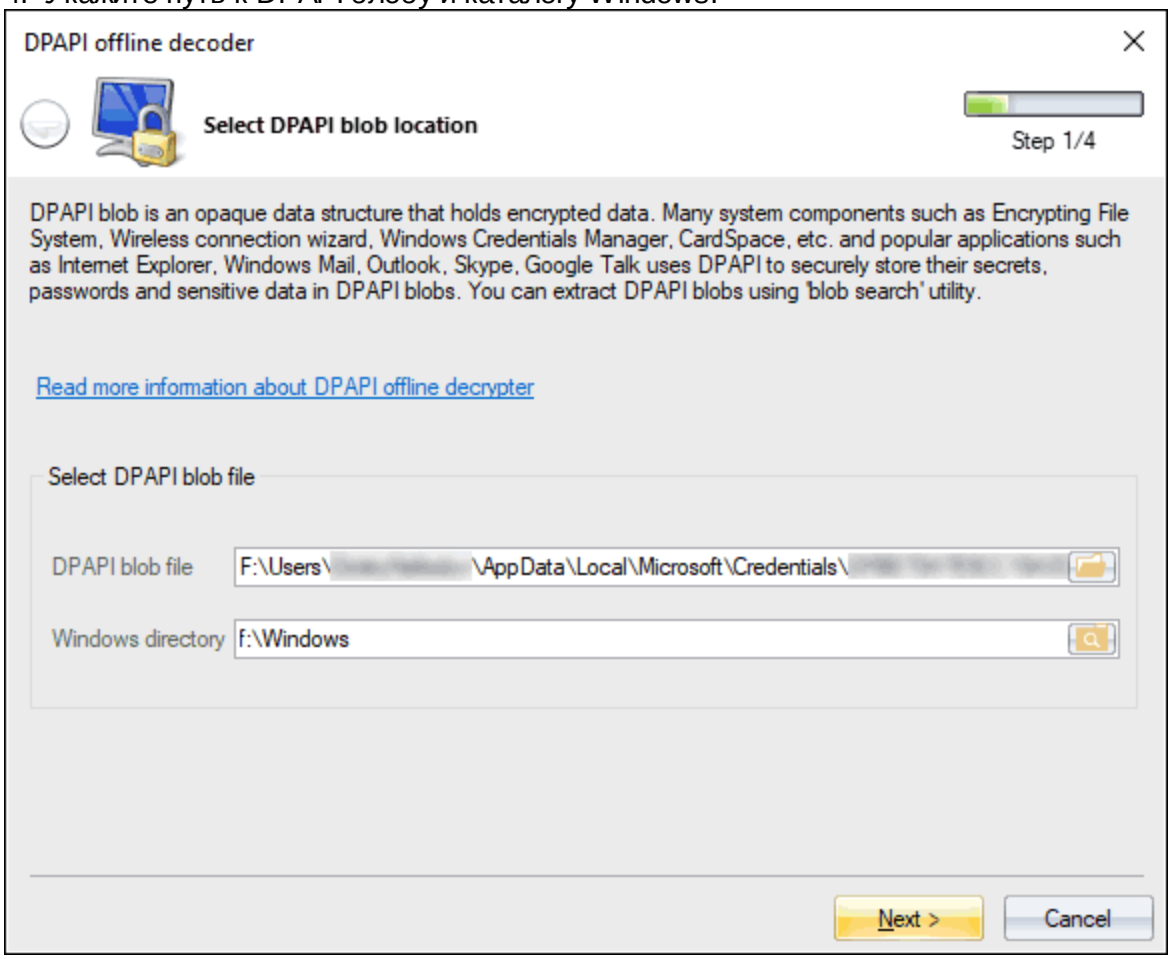
Пошаговая инструкция для расшифровки DPAPI без знания пароля.

1. Убедитесь, что для учетной записи, данные которой необходимо расшифровать, настроен биометрический вход.

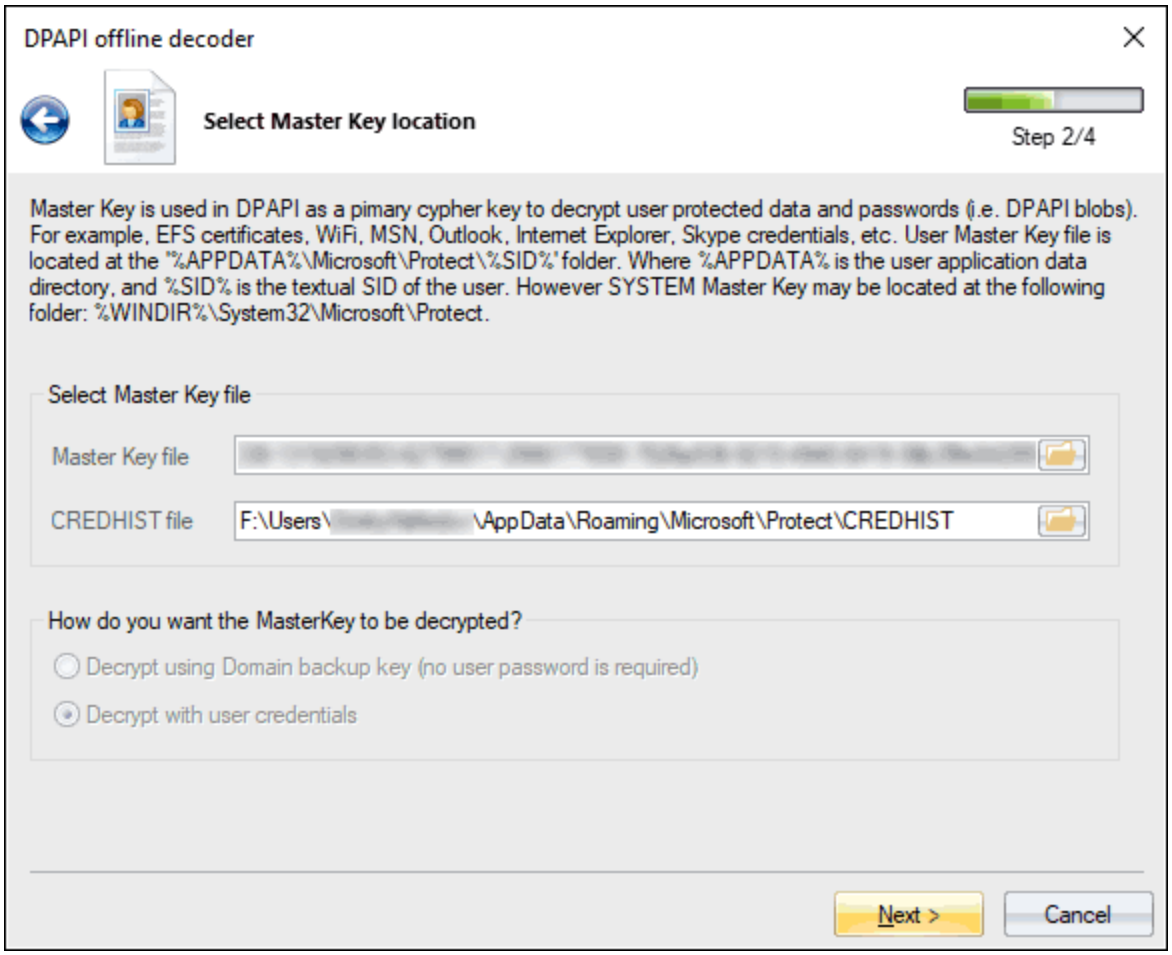
2. Подключите диск с учетной записью в вашему ПК. Если это виртуальный диск, например от виртуальной ОС, то он должен быть доступен для записи. В противном случае, программа не сможет прочитать данные из каталога Windows Hello.

3. Запустите программу Windows Password Recovery, в меню Utils выберите DPAPI decoder and analyzer -> Decrypt DPAPI data blob

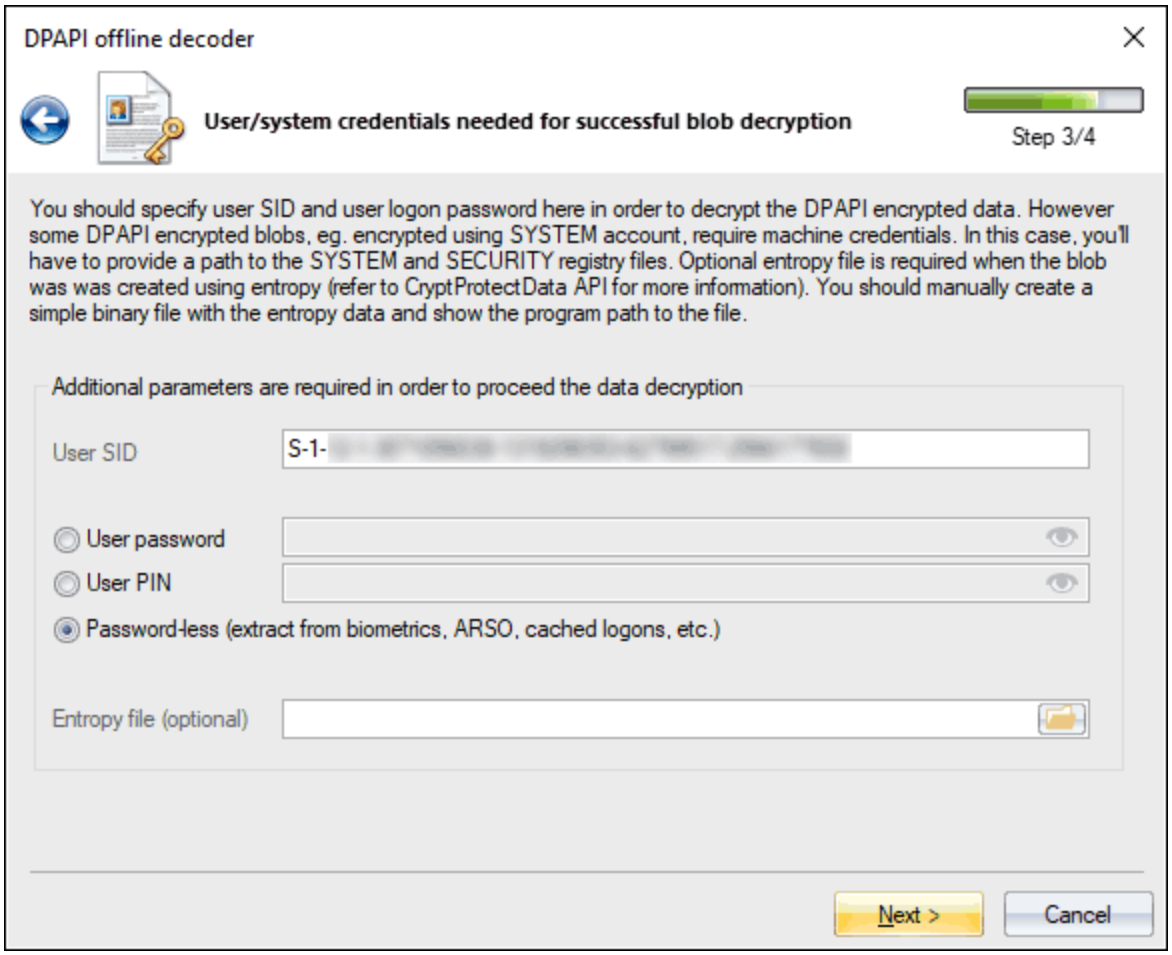
4. Укажите путь к DPAPI блобу и каталогу Windows.

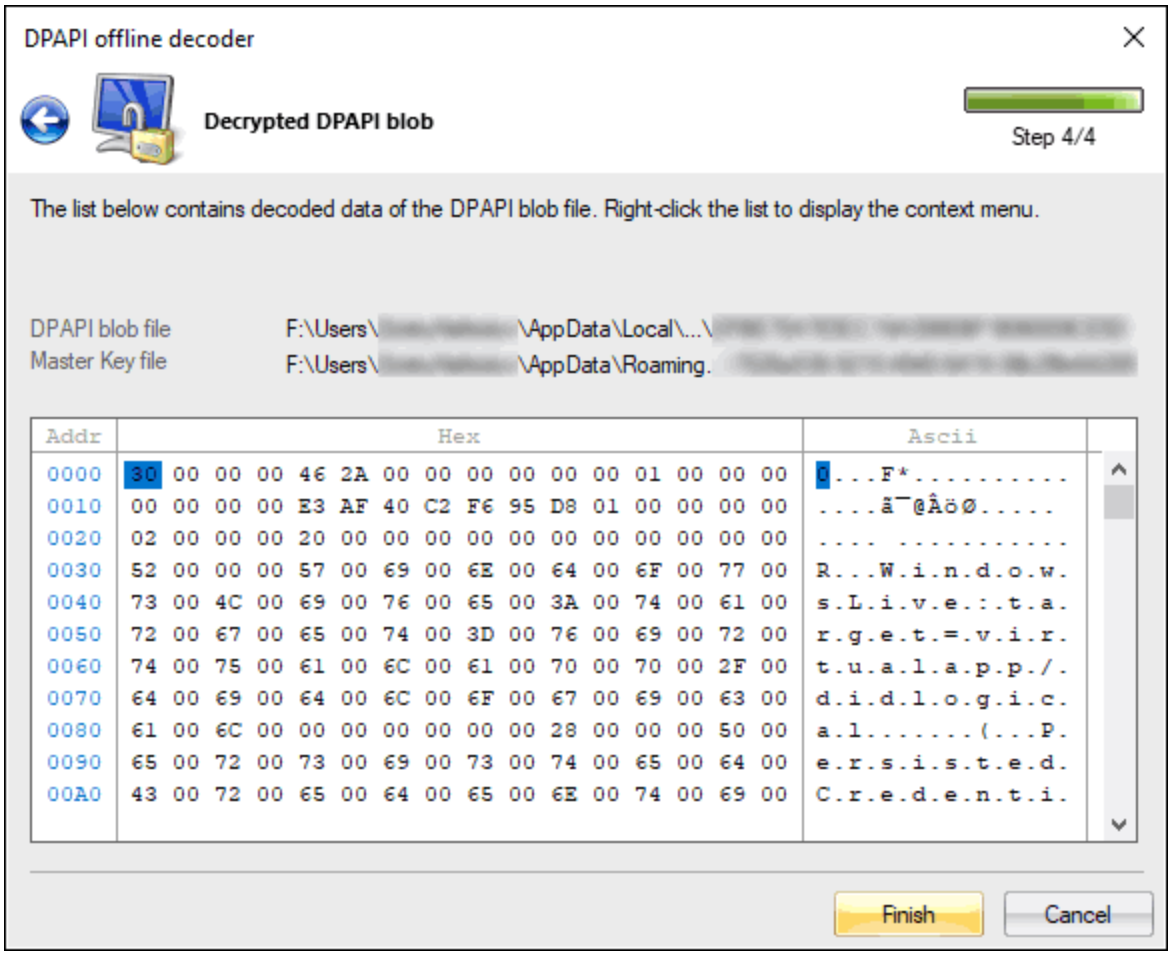


5. В следующем диалоге укажите путь к мастер ключу пользователя.



6. Теперь выберите тип расшифровки 'без пароля' и нажмите *Next* чтобы расшифровать DPAPI блоб.





1.8 Выводы

Несмотря на все заверения Microsoft о безопасности биометрической аутентификации Windows Hello, мы видим, что это, мягко выражаясь, не совсем так.

Если у вас настроен биометрический вход в систему и отключена защита TPM, будьте предельно осторожны. Все ваши персональные данные в потенциальной опасности!

Для их защиты мы рекомендуем одно из следующих: настроить шифрование диска, включить защиту TPM (если ваше оборудование ее поддерживает) или отказаться от биометрии.