Win2K, Win2K3, Windows Server 2008 और Windows Server 2012 में DPAPI डेटा सुरक्षा की कमजोरी

© 2021 पास्केप सोफ्टवेर (हिन्दी अनुवाद : धीरेन कुमार)
पास्केप सोफ्टवेर (हिन्दी अनुवाद : धीरेन कुमार)

1. कमजोरी का संक्षिप्त विवरण 3
1.1 समस्या 4
1.2 प्रभावित सॉफ्टवेयर 4
2. तकनीकी जानकारी 5
2.1 Windows XP और उच्चतर OSes में DPAPI एन्क्रिप्शन 6
2.2 Windows 2000 OS में DPAPI एन्क्रिप्शन 6
2.3 Windows 2003, 2008, 2012 server OSes में DPAPI एन्क्रिप्शन दोष 7
3. कमजोरी का उपयोग करना 9
3.1 Windows 2012 server में इंटरेक्टिव डोमेन यूजर बनाना 10
3.2 नए यूजर के लिए मास्टर की और DPAPI सीक्रेट बनाना 10
3.3 मालिक के लॉगऑन पासवर्ड को जाने बिना यूजर DPAPI सीक्रेट को डिक्रिप्ट करना 10
4. निष्कर्ष 15
Index 0

कमजोरी का संक्षिप्त विवरण

1 कमजोरी का संक्षिप्त विवरण

1.1 समस्या

हमारे पिछले लेखों में से एक DPAPI प्रणाली के ऑपरेटिंग सिद्धांतों, इसकी असाधारण विश्वसनीयता, कार्यात्मक मूल्य और क्रैकिंग प्रतिरोध का वर्णन करता है। कुछ समय पहले, हमें कभी-कभी पता चला कि Windows 2003 में कुछ DPAPI ब्लॉब्स में डिक्रिप्शन समस्याएँ थीं। समस्या का कारण निर्धारित करने के बाद, DPAPI सुरक्षा में एक दिलचस्प उल्लंघन का पता चला था जिसे सभी सर्वर ऑपरेटिंग सिस्टम में पुन: पेश किया जा सकता है, Win2K से शुरू होकर Windows Server 2012 के साथ समाप्त होता है।

संक्षेप में, इसका सार निम्नलिखित है: डिफ़ॉल्ट रूप से, इंटरेक्टिव लॉगऑन विशेषाधिकार वाले सभी डोमेन उपयोगकर्ताओं की मास्टर कीज, बिल्ट-इन अकाउन्ट्स को छोड़कर, Windows 2000 कम्पेबिलिटी मोड में बनाई जाती हैं; इसलिए, DPAPI के साथ एन्क्रिप्ट किए गए डेटा के डिक्रिप्शन के लिए मालिक के लॉगऑन पासवर्ड की आवश्यकता नहीं होती है।

1.2 प्रभावित सॉफ्टवेयर

इसका अर्थ यह है कि कोई भी एडमिनिस्ट्रेटर या कोई अन्य यूजर्स जिसके पास सर्वर तक भौतिक पहुंच है, वह कमजोर यूजर अकाउन्ट्स के निम्नलिखित व्यक्तिगत डेटा को डिक्रिप्ट कर सकता है:

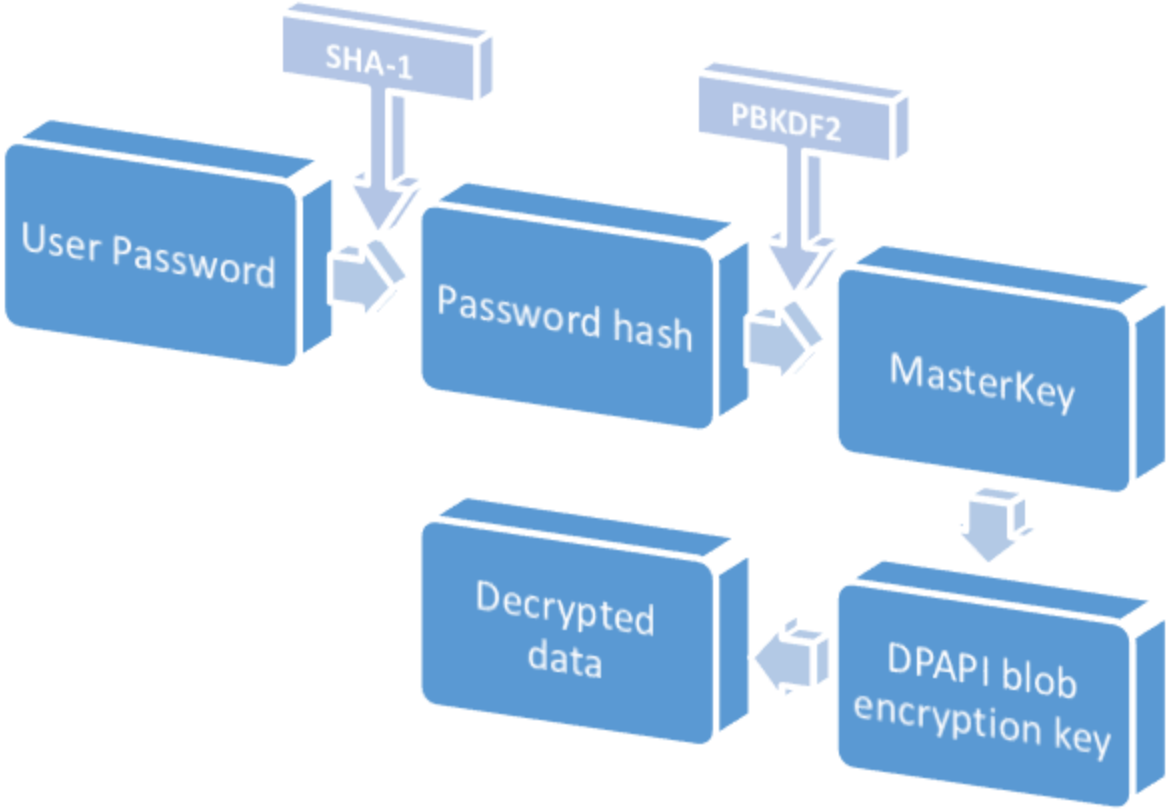
- लोकप्रिय ब्राउज़रों में पासवर्ड और फॉर्म ऑटो-कोम्प्लेशन डेटा: Internet Explorer, Google Chrome, Opera Browser, आदि।
- Outlook, Windows Mail, Windows Live Mail आदि में ई-मेल अकाउंट पासवर्ड।
- Windows FTP manager के अकाउन्ट पासवर्ड
- शेर किए गए फ़ोल्डरों और संसाधनों के पासवर्ड एक्सेस कर सकता है
- वायरलेस नेटवर्क की कीज और पासवर्ड
- Windows CardSpace की एन्क्रिप्शन कीज
- Windows Vault में एन्क्रिप्शन कीज
- रिमोट डेस्कटॉप कनेक्शन पासवर्ड
- .NET पासपोर्ट पासवर्ड
- Windows Live ID व्यक्तिगत डेटा
- फ़ाइल सिस्टम को एन्क्रिप्ट करने वाली प्राइवेट की (EFS)
- S-MIME मेल में एन्क्रिप्शन कीज
- यूजर सर्टिफिकेट
- इंटरनेट सूचना सेवाओं में निजी डेटा
- EAP/TLS और 802.1x प्रमाणीकरण
- क्रेडेंशियल मैनेजर में नेटवर्क पासवर्ड
- किसी भी एप्लिकेशन में व्यक्तिगत डेटा, प्रोग्रामेटिक रूप से विंडोज API फ़ंक्शन CryptProtectData, जैसे Skype, Windows Rights Management Services, Windows Media, MSN messenger, Google Talk, आदि के साथ सुरक्षित।

तकनीकी जानकारी

2 तकनीकी जानकारी

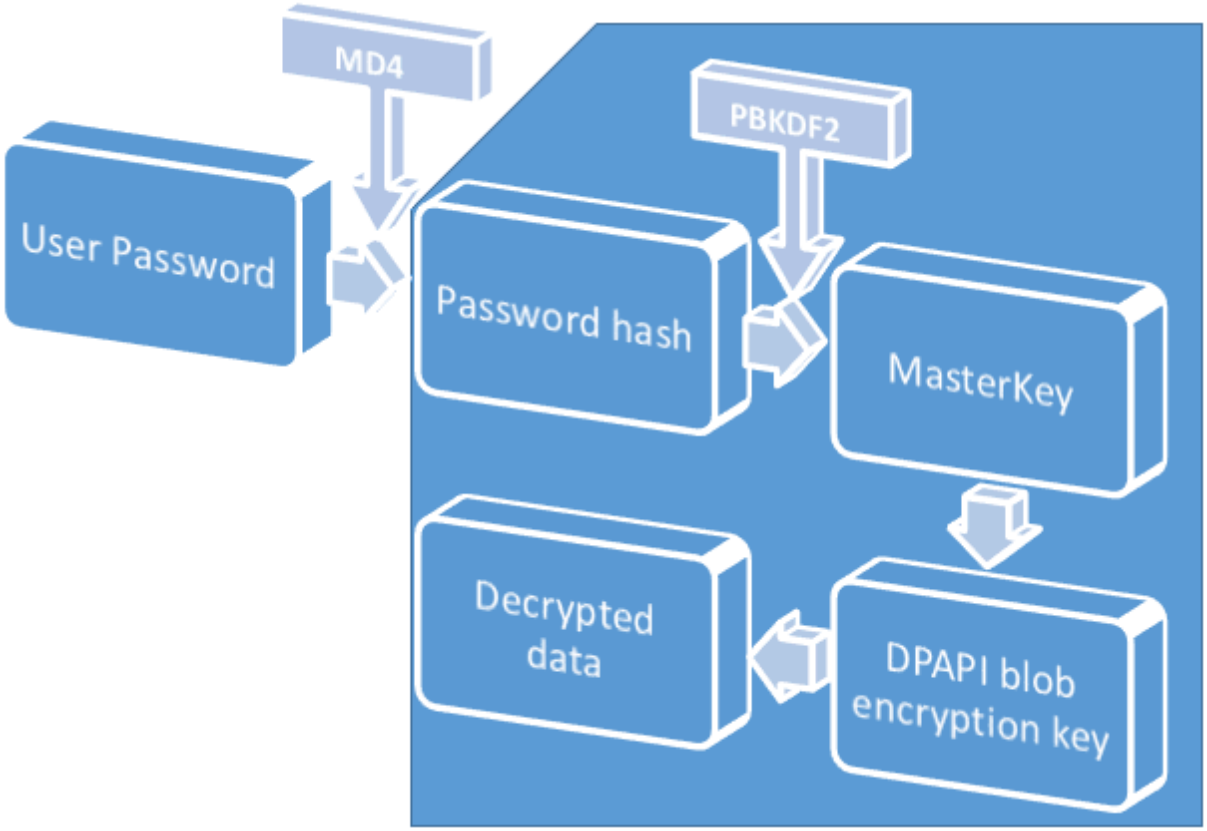
2.1 Windows XP और उच्चतर OSes में DPAPI एन्क्रिप्शन

DPAPI के साथ एन्क्रिप्टेड निजी डेटा को डिक्रिप्ट करने की प्रक्रिया इस तरह दिखती है (कुछ विवरण छोड़े गए हैं): प्रारंभ में, पासवर्ड हैश प्राप्त करने के लिए डेटा मालिक के लॉगऑन पासवर्ड को SHA-1 के माध्यम से पारित किया जाता है; पासवर्ड हैश और मालिक के SID को तब PBKDF2 फ़ंक्शन में फीड किया जाता है। आउटपुट पर, वह एक प्रीकी उत्पन्न करता है, जो मास्टर की के डिक्रिप्शन में भाग लेता है। इसके बदले में डिक्रिप्टेड मास्टर की का उपयोग वास्तविक DPAPI ब्लॉब्स के डिक्रिप्शन के लिए किया जाता है। यहाँ यह एक चार्ट में कैसा दिखता है:



2.2 Windows 2000 OS में DPAPI एन्क्रिप्शन

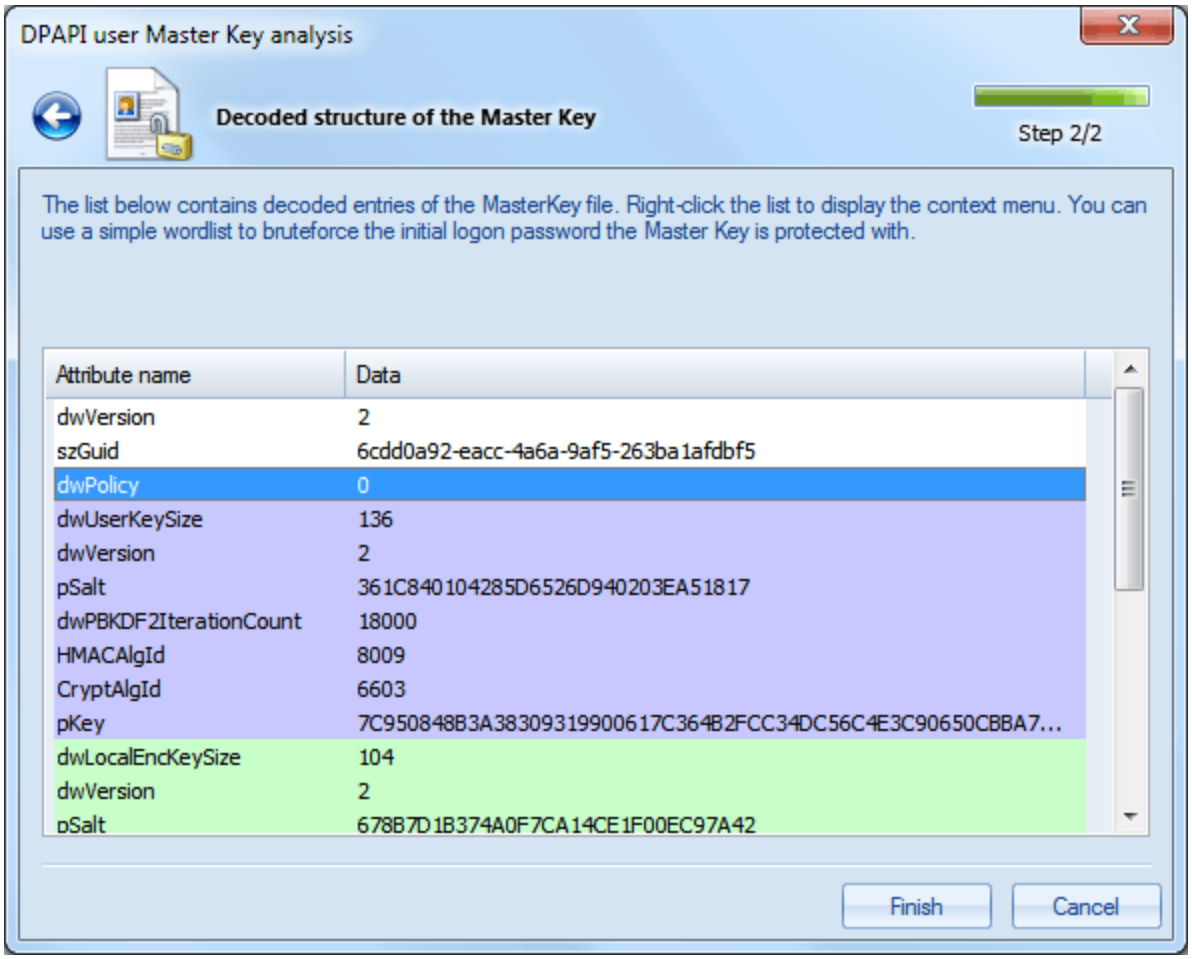
Windows 2000 में प्रयुक्त DPAPI के पहले कार्यान्वयन में अन्य मास्टर की एन्क्रिप्शन एल्गोरिदम थे। लेकिन ऐसा नहीं था जिसने इसे बेहद कमजोर बना दिया था; यह तथ्य था कि यूजर का पासवर्ड हैश प्राप्त करने के लिए, उसने SHA-1 के बजाय MD4 हैशिंग फ़ंक्शन का उपयोग किया। यहां है कि यह कैसा लग रहा है:



मनोरंजक रूप से, उसी हैशिंग फ़ंक्शन का उपयोग यूजर्स के लॉगऑन पासवर्ड को मान्य करने में भी किया जाता है, जिसके हैश या तो SAM रजिस्ट्री में या Active Directory (सर्वर ऑपरेटिंग सिस्टम के लिए) में संग्रहीत होते हैं। इस प्रकार, मास्टर की को डिक्रिप्ट करने के लिए उपयोगकर्ता का प्लेनटेक्स्ट पासवर्ड वास्तव में आवश्यक नहीं है। SAM या NTDS.DIT से संबंधित उपयोगकर्ता के मौजूदा MD4 हैश को लेना और इसे डेटा-इन के रूप में उपयोग करना पर्याप्त है। बाकी सब पहले से ही पता है।

2.3 Windows 2003, 2008, 2012 server OSes में DPAPI एन्क्रिप्शन दोष

कौन सा एल्गोरिथम प्रयोग किया जाता है - SHA-1 या MD4 - मास्टर की के हेडर में निर्दिष्ट है। dwPolicy फलेग का बिट 4 इंगित करता है कि मास्टर की SHA-1 एल्गोरिथम का उपयोग करती है। Windows सर्वर OSes में सहभागी लॉगऑन विशेषाधिकार वाले नव निर्मित यूजर्स के पास यह फ़्लैग डिफ़ॉल्ट रूप से सेट नहीं होता है। क्रमशः, उनके निजी डेटा के डिक्रिप्शन के लिए लॉगऑन पासवर्ड की आवश्यकता नहीं होती है।


DPAPI user Master Key analysis
Decoded structure of the Master Key
Step 2/2
The list below contains decoded entries of the MasterKey file. Right-click the list to display the context menu. You can use a simple wordlist to bruteforce the initial logon password the Master Key is protected with.
Attribute name
Data
dwVersion 2
szGuid 6cdd0a92-eacc-4a6a-9af5-263ba1afdbf5
dwPolicy 0
dwUserKeySize 136
dwVersion 2
pSalt 361C840104285D6526D940203EA51817
dwPBKDF2IterationCount 18000
HMACAlgId 8009
CryptAlgId 6603
pKey 7C950848B3A38309319900617C364B2FCC34DC56C4E3C90650CBBA7...
dwLocalEncKeySize 104
dwVersion 2
pSalt 678B7D1B374A0F7CA14CE1F00EC97A42
Finish
Cancel

कमजोरी का उपयोग करना

3 कमजोरी का उपयोग करना

3.1 Windows 2012 server में इंटरेक्टिव डोमेन यूजर बनाना

आइए सिद्धांत से अभ्यास की ओर बढ़ते हैं और Windows Server 2012 डोमेन में एक नया यूजर जोड़ने का प्रयास करते हैं, फिर कुछ DPAPI सीक्रेट बनाते हैं और फिर मालिक के लॉगऑन पासवर्ड के बिना इसे ऑफ़लाइन डिक्रिप्ट करते हैं।

"Active Directory यूजर्स और कंप्यूटर" कंसोल खोलें और टेस्ट नामक एक नया डोमेन उपयोगकर्ता बनाएं। उस उपयोगकर्ता को एक सहभागी लॉगऑन विशेषाधिकार प्रदान करें। ऐसा करने के लिए, आप बस उस उपयोगकर्ता को लोकल एडमिनिस्ट्रेटर ग्रुप में जोड़ सकते हैं।

3.2 नए यूजर के लिए मास्टर की और DPAPI सीक्रेट बनाना

अब हमें सिस्टम को लॉग ऑफ करना होगा और फिर इस अकाउन्ट के तहत लॉगऑन करना होगा। नए अकाउन्मेंट अभी तक मास्टर की नहीं है। इसे CryptProtectData फ़ंक्शन की पहली कॉल के दौरान बनाया जाएगा। हम संबंधित फ़ंक्शन के लिए कॉल को बाध्य करके उस प्रक्रिया को गति देंगे। उस प्रयोजन के लिए, हमारे पास एक समान नाम वाली यूटिलिटी CryptProtectData.exe है, जो केवल API फ़ंक्शन CryptProtectData को कमांड-लाइन मापदंडों के साथ कॉल करती है (यूटिलिटी सोर्स कोड वेबसाइट पर उपलब्ध है)। इसे निम्न पैरामीटर के साथ लॉन्च करें: CryptProtectData mysupersecret out.dat। आउटपुट पर, हमारे पास एक DPAPI ब्लॉब के साथ out.dat फ़ाइल होगी जिसमें हमारा एन्क्रिप्टेड टेक्स्ट (mysupersecret) होगा।

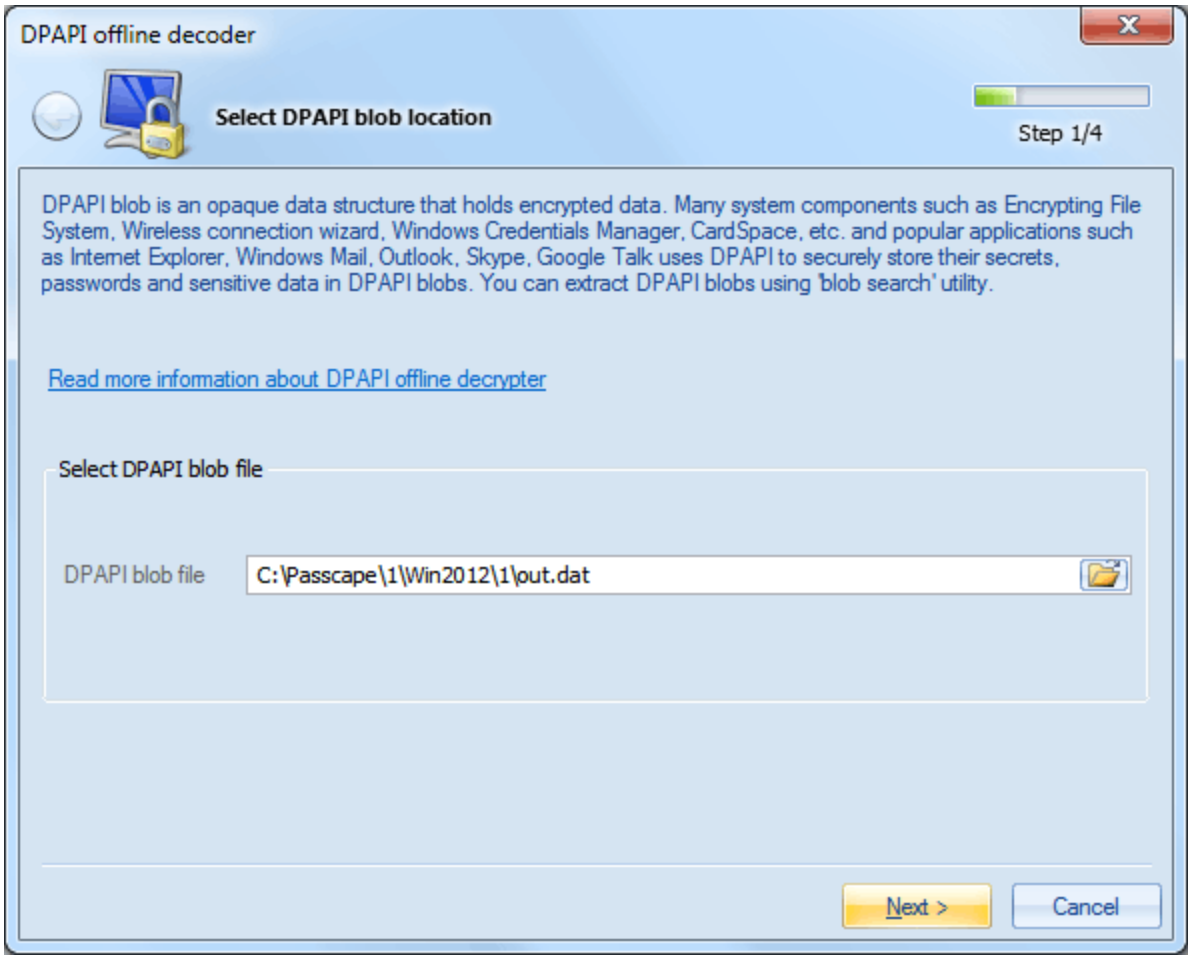
तो, मास्टर की को फ़ोल्डर में बनाया और संग्रहीत किया गया है
C:\Users\test\AppData\Roaming\Microsoft\Protect\<SID>\<mk>
जहाँ <SID> - मालिक का पक्ष। हमें अभी भी इसकी आवश्यकता होगी, इसलिए या तो इसे याद रखें या संपूर्ण कैटलॉग को कॉपी करें।
<mk> - DPAPI मास्टर की का नाम; उदा., 6cdd0a92-eacc-4a6a-9af5-263ba1afdbf5

इसके अलावा, out.dat फ़ाइल के ऑफ़लाइन डिक्रिप्शन के लिए हमें डेटा मालिक के MD4 हैश की आवश्यकता होगी, जो Active Directory में संग्रहीत है। इसे प्राप्त करने के लिए, हम अपनी यूटिलिटी का लाभ उठाएँगे और NTDS.DIT फ़ाइल की एक कोपी बनाएगें, साथ ही हैश प्राप्त करने के लिए आवश्यक सिस्टम रजिस्ट्री की एक कोपी बनाएँगे।

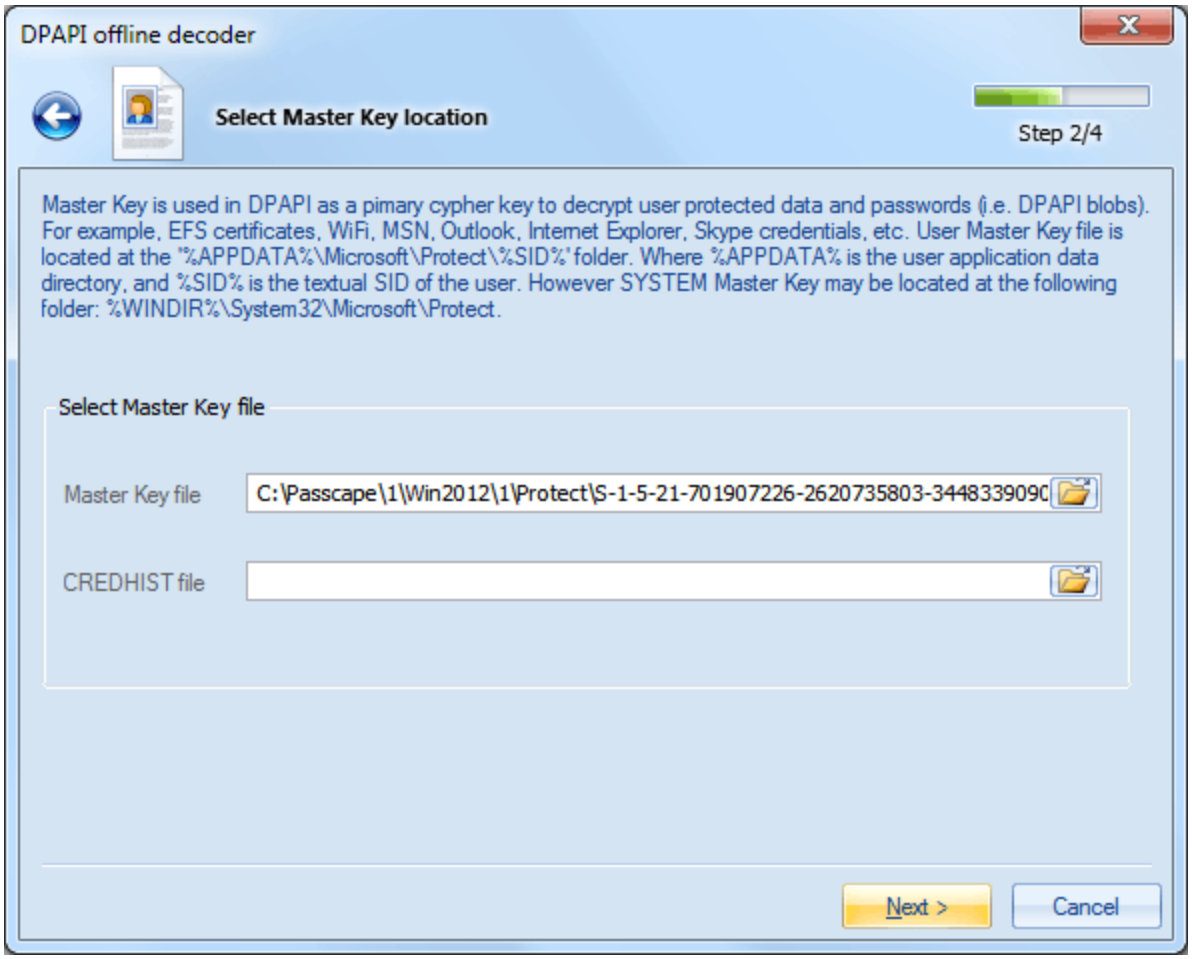
3.3 मालिक के लॉगऑन पासवर्ड को जाने बिना यूजर DPAPI सीक्रेट को डिक्रिप्ट करना

परिणामस्वरूप, हमारे पास होगा:

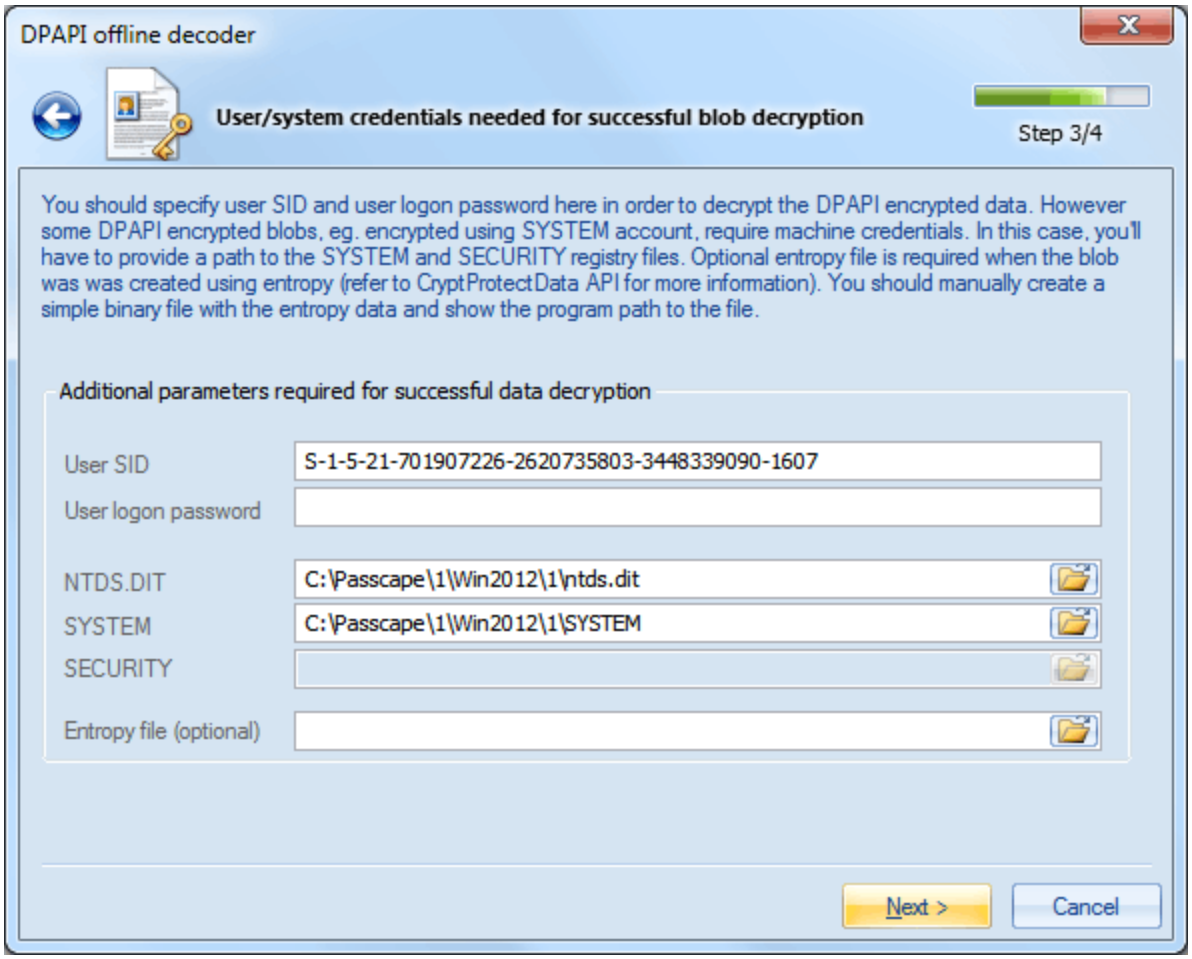
- एन्क्रिप्टेड रहस्य के साथ out.dat फ़ाइल, जिसे हमें डिक्रिप्ट करने की आवश्यकता है
- डेटा मालिक का टेक्स्ट SID
- उनकी मास्टर की
- मालिक का हैश (फाइलें NTDS.DIT और SYSTEM)।



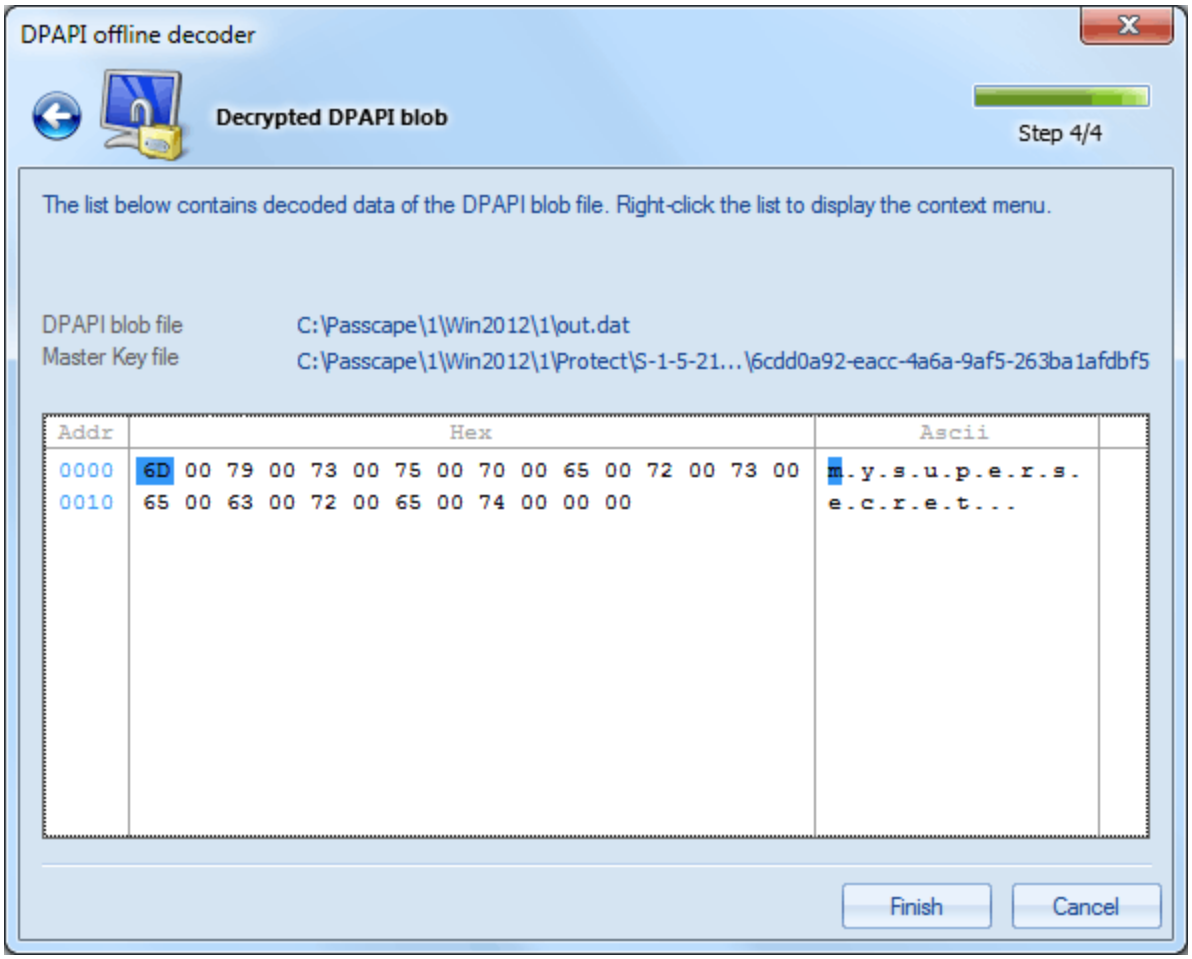
अब, DPAPI ऑफ़लाइन डिक्रिप्शन यूटिलिटी लॉन्च करें और इसे out.dat फ़ाइल का पाथ बताएं।



विज़ार्ड के दूसरे चरण पर, डेटा मालिक की मास्टर की के लिए पाथ निर्दिष्ट करें: पाथ का चयन करें और फिर अगला क्लिक करें। कार्यक्रम एक चेतावनी देता है कि मास्टर की में एक कमजोरी पाई जाती है, और इसलिए डिक्रिप्शन दो तरीकों से किया जा सकता है: उपयोगकर्ता के पासवर्ड के साथ और इसके बिना। हम, निश्चित रूप से, बाद वाला चाहते हैं।



इसलिए, विज़ार्ड के अगले चरण पर, पासवर्ड फ़ील्ड को खाली छोड़कर, मालिक का SID और NTDS.DIT और सिस्टम फ़ाइलों का पाथ दर्ज करें।



अगला क्लिक करें, और यहां हमारे पास डिक्रिप्टेड रहस्य है। जैसा कि आप देख सकते हैं, मालिक का पासवर्ड आवश्यक नहीं था।

निष्कर्ष

4 निष्कर्ष

जो बात पूरी तरह से स्पष्ट नहीं है वह यह है कि क्या इंटरैक्टिव यूजर्स में यह दोष किसी त्रुटि से संबंधित है या इसे इस तरह नहीं माना जाना चाहिए। शायद यह सर्वर ऑपरेटिंग सिस्टम में DPAPI कार्यान्वयन की एक ख़ासियत है; उदाहरण के लिए, पिछड़ी संगतता प्रदान करने के लिए। दूसरी ओर, यह अत्यधिक असंभव प्रतीत होता है, क्योंकि यूजर्स के गोपनीय डेटा की सुरक्षा ठीक से सुनिश्चित नहीं की जाती है, जबकि DPAPI को विशेष रूप से मालिक के पासवर्ड के आधार पर डेटा सुरक्षा प्रणाली के लिए बनाया गया था। अजीब बात है, लेकिन यह पता चला है कि सर्वर ऑपरेटिंग सिस्टम चलाने वालों की तुलना में डेस्कटॉप पीसी ऑफ़लाइन पासवर्ड पुनर्प्राप्ति के लिए अधिक प्रतिरोधी हैं। एक तरह से या दूसरे, सिस्टम एडमिनिस्ट्रेटर्स को इस कमजोरी के बारे में पता होना चाहिए, जैसा कि पहले से चेतावनी दी गई है।