

DPAPI Windows

10

© 2019 Passcape Software
Passcape Software

1.	DPAPI Windows 10	3
1.1	3
1.2	3
1.3	DPAPI	3
1.4	DPAPI	3
1.5	Automatic Restart Sign-On (ARSO)	4
1.6	Trusted Boot Auto-Logon (TBAL)	4
1.7	TBAL	5
1.8	5
1.9	6
1.10	PoC	6
1.11	6

1

DPAPI Windows 10

1.1

DPAPI,
Windows 10.

1.2

Microsoft Windows 10, 1709 (Fall Creators Update),
Windows 10,

1.3

DPAPI

Data Protection Application Programming Interface DPAPI -
Windows, Windows 2000. DPAPI
- , : CryptProtectData
CryptUnprotectData.
CryptProtectData/CryptUnprotectData
DPAPI .

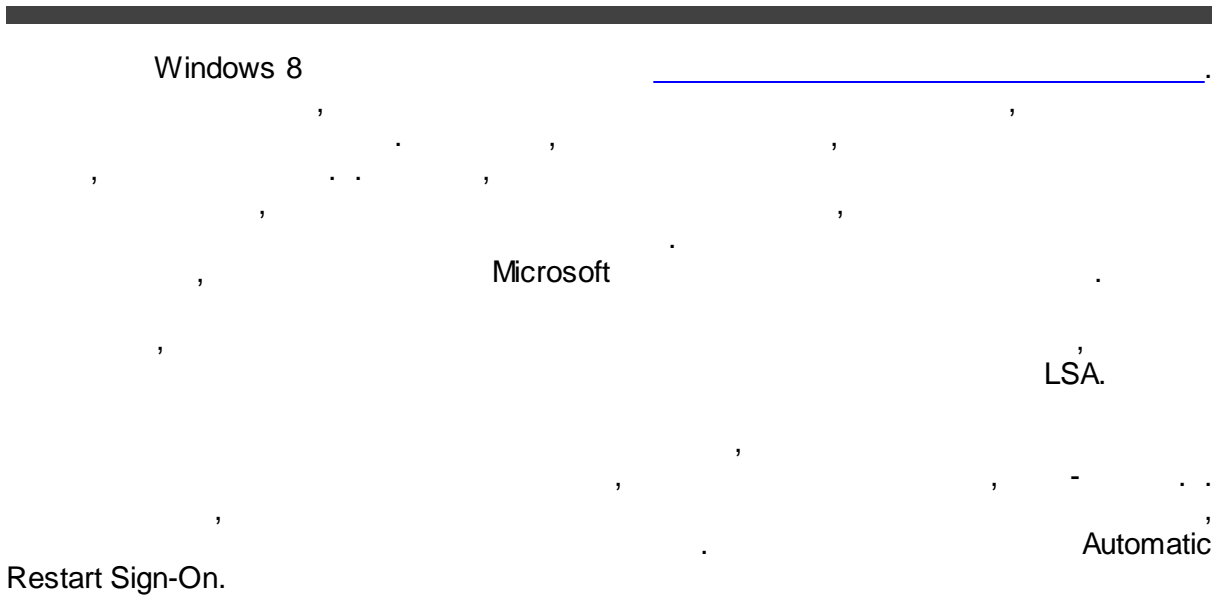
1.4

DPAPI

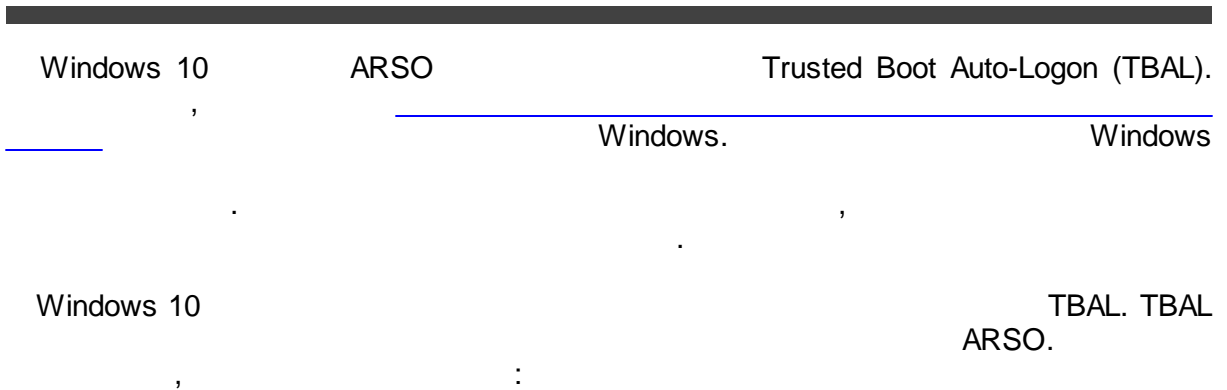
DPAPI - , ,
DPAPI , DPAPI
NTLM , DPAPI
NTLM , SAM,
DPAPI.
Microsoft
DPAPI,

- DPAPI
- DPAPI,
- DPAPI,

1.5 Automatic Restart Sign-On (ARSO)



1.6 Trusted Boot Auto-Logon (TBAL)



- Microsoft
- TBAL
- Windows 10, TBAL
- TBAL?

1.7

TBAL

Windows 10 LSA
DefaultPassword _TBAL_{68EDDCF5-0AEB-4C28-A770-
 AF5302ECA3C9},
 TBAL.
 LSA
M\$_MSV1_0_TBAL_PRIMARY_{22BE8E5B-58B3-4A87-BA71-41B0ECF3A9EA},
 NTLM SHA1
 Microsoft,
M\$_CLOUDAP_TBAL_{8283D8D4-55B6-466F-B7D7-17A1352D9CAB}_<UID>
 (Windows 1607) **M\$_CLOUDAP_TBAL_{4416F0BD-3A59-4590-9579-
 DA6E08AF19B3}_<UID>**, <UID> SHA256
 96-
 DPAPI.
 DPAPI TBAL
 SHA1 (),
 96- Microsoft. LSA-
 . TBAL

1.8

DPAPI , TBAL
 DPAPI ,
 DPAPI ,
 DPAPI
 Microsoft ,
 Windows. ,

1.9

- Google Chrome, Internet Explorer, Microsoft Edge, Opera
- Microsoft Office Outlook, Windows Mail
- [Windows Vault](#)
- (EFS)
- S-MIME
- [Credential Manager](#)
- DPAPI, Skype, Windows Rights Management Services, Windows Media, Google Talk

1.10 PoC

Windows Vault, Facebook, DPAPI

1.11

Windows

Windows 10 1709 SYSKEY-