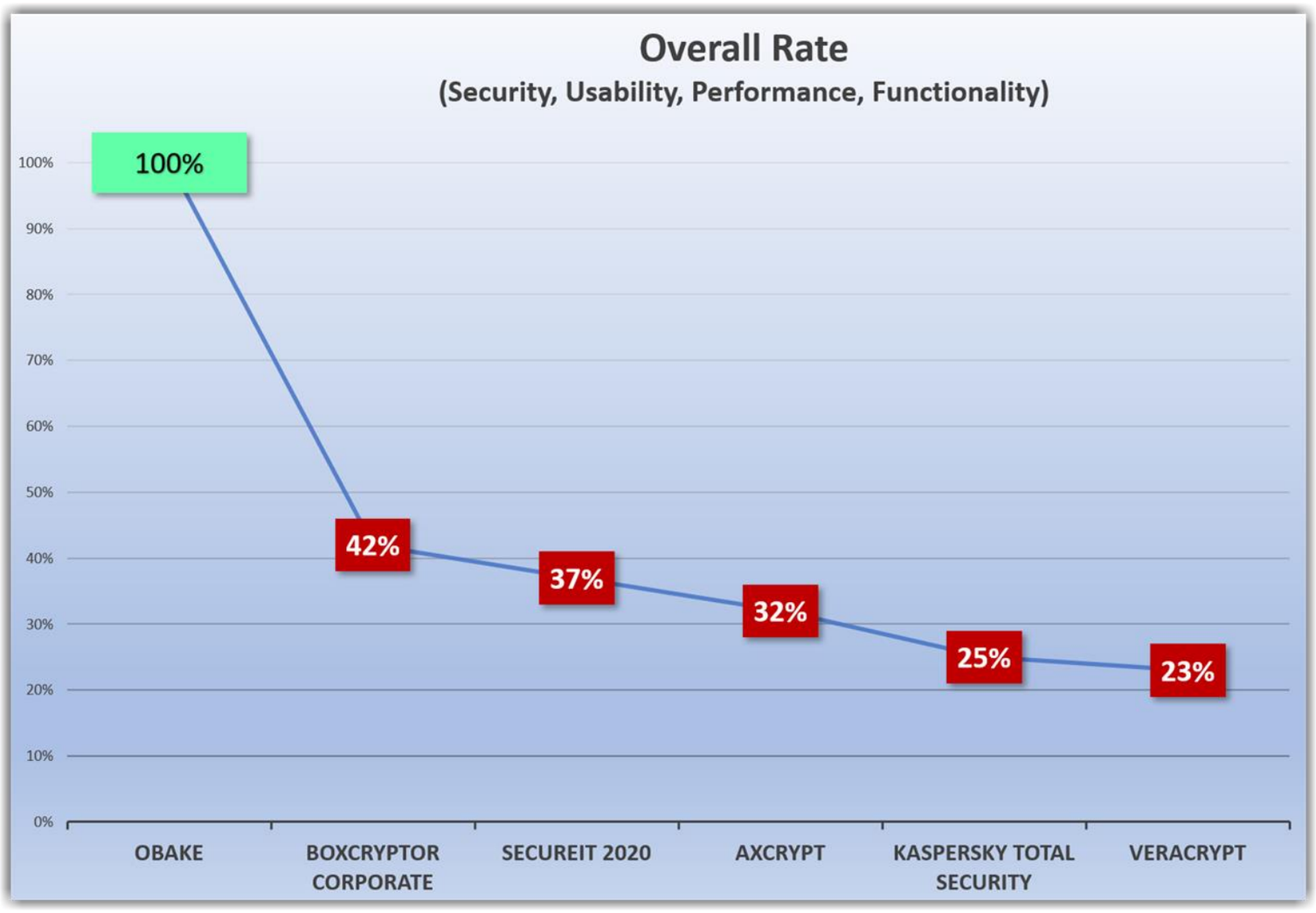
OBAKE

The Easiest and Powerful Encryption Suite for MS-Windows

COMPARATIVE TABLE 2023

Best Folder/File Encryption Software



FEATURES	OBAKE	Boxcryptor Corporate	SecureIT 2020	AxCrypt	Kaspersky Total Security	VeraCrypt
	100 %	42 %	37 %	32 %	26 %	23 %
Great usability and easiness	✓	✓	✓	✓	✓	✓ [1]
No file quantity limit	✓	✓	✓	✓	✓	✓
Handles files larger than 4Gb on 32-bit systems	✓	✓	✓	✓	✓	✓
Works on Folders and Subfolders	✓	✓	✓		✓ [2]	
DIGITAL CERTIFICATES						
Encrypts data using Digital Certificates	✓	✓				
Certificate: maximum bit-size	8192 bits	4096 bits				
Certificate Type	X509v3	RSA				
Works with ICP-BR chain	✓	✓				
Accepts Certificates from Public CA's	✓	✓				
Accepts Certificates from Private CA's	✓	✓				
Import and export certificates easily	✓	✓		✓		
Certificates safely stored on the user's machine	✓	✓ [3]		✓ [3]		
User certificate is access-protected	✓	✓ [33]		[8]		
Accepts Certificates in the local Windows Store	✓	[28]				
Works with Self-Signed Certificates	✓	✓				
Enables TimeStamp with choice of servers	✓					
Unlimited number of Public Keys (or recipients)	✓	✓		✓		
SECRET KEYWORDS						
Encrypts data using a secret key	✓ [4]		✓	✓ [5]	✓	✓
Requires the secret key at each file opening	✓		✓	[6]	✓ [7]	✓ [5]
Set different random keys per file on multiple files	✓		✓ [6]			
FUNCTIONALITY AND SECURITY						
Allows encrypted file sharing	✓	✓	✓	✓ [8]		✓ [9]
Allows direct sharing w/o any manufacturer's link or procedure	✓	[28]	✓	[8]	✓	
Sharing by Digital Certificates (Public Keys)	✓	✓ [28]				
Share/Auth data are embedded in files [42]	✓	[29]				
Checks encrypted file after encryption	✓					
Allows to check the creator and the authorized persons in files	✓	✓ [28]				
Allows to verify file's Integrity, Authenticity and Origin	✓	✓ [28]				
Sanitizes input file automatically	✓		✓	✓		
Deletes input file automatically	✓	✓	✓	✓	✓	
Allows customized and intelligent files compression	✓		✓			✓
Allows you to cancel the operation at any time	✓	✓	✓			
Allows to quickly open/edit encrypted files (fast-open) [12]	✓	✓		✓	✓ [13]	✓ [13]
Automatically re-encrypts when closing a file	✓	✓		✓		
Allows to keep the file's original date/time	✓	✓	✓	✓	✓	✓
Does not require an exclusive secure folder	✓		✓	✓		
Does not require data-vault [14]	✓		✓	✓		
Does not require online services and logins	✓	[31]	✓		✓	✓
Does not allow data opening on smartphones	✓		✓		✓	
Allows a password for the program access	✓	✓ [38]			✓	
Allows 2FA for the program access (Google Authenticator)	✓	✓ [39]				
Zero-Knowledge compliant	✓	✓ [32]	✓			✓
Enables access restriction to critical settings [15]	✓	✓ [32]			✓	
Enables secure access to the settings restrictions [16]	✓	✓ [32]			✓ [17]	
Enables mandatory sharing by code [18]	✓					

OBAKE

The Easiest and Powerful Encryption Suite for MS-Windows

COMPARATIVE TABLE 2023

Best Folder/File Encryption Software

Enables mandatory sharing by capillarity [19]	✓	✓ [41]				
Enables email log for critical configuration changes [20]	✓	✓			✓	
Allows the creation of "User Groups" to share	✓	✓				
Allows the creation of "User Groups" without a common key [35]	✓					
Integration with Microsoft-365 [33]	✓					
Integration with Windows Explorer / Files Explorer	✓	✓		✓		✓
Allows “end-to-end” synchronization with One-Drive	✓	✓ [37]	✓	✓		
Allows “end-to-end” synchronization with Google-Drive	✓	✓ [37]	✓	✓		
Allows “end-to-end” synchronization with Dropbox	✓	✓ [37]	✓	✓		
Passwords and Keys are independent	✓	[21]				
ADMIN-authorization free – no privileged accesses	✓	[32]	✓			✓
Allows revocation/exchange of authorizations	✓	✓		✓		
Protected against hacking/code injection	✓	✓ [40]	✓	?	✓	?
Protected against Disassembly	✓	✓ [40]	✓	?	✓	?
Protected against code-hijacking	✓	✓ [40]	✓	?	✓	?
ALGORITHMS						
Has algorithms for compliance (AES)	✓	✓	✓	✓	✓	✓
Has AES-NI by hardware (top performance) [43]	✓					
Has AES-XTS for compliance IEEE	✓					✓
Has strong modern algorithms (XSalsa, ChaCha, Poly305, etc.) [44]	✓					
Symmetric "military-grade" algorithm (> 256 bits)	✓		✓ [22]			
Calculated One-Time keys	✓ [24]	✓ [34]				
Symmetric encryption key length	**32-65536 bits**	256 bits	448 bits	256 bits	56 bits	256 bits
HASH size	**512 bits**	512 bits		256 bits		256 bits
Derivations of the main Key [36]	5 [23]	2	1	1	1	1
PERFORMANCE						
OBAKE algorithm: Encryption (2.39Gb) [25] [36]	**7,9 s**	22 s	154s	150 s	25 s	24 s
OBAKE algorithm: Decryption (2.39Gb) [36]	**7,7 s**	11,5 s	68s	55 s	9 s	21 s
AES-NI algorithm: Encryption (2.39Gb) [25] [36]	**4,3 s**	22 s	154s	150 s	25 s	24 s
AES-NI algorithm: Decryption (2.39Gb) [36]	**4,8 s**	11,5 s	68s	55 s	9 s	21 s
Additional Features						
Compliance with GDPR, LGPD, and other laws	✓	✓		✓	✓ [26]	✓
Compliance with NIST-FIPS, ISO-IEC, RTF	✓	✓		✓	✓ [26]	✓
Resistant to Monitoring/Data-Inspection Laws	✓			✓		✓
Allows the source-code auditing	✓			✓		✓
Companies can customize algorithms	✓					
	77	**32.5**	**28.5**	**24.5**	**20**	**18**

✓ = 1 ✓ = 0,5

1. The configuration/installation process must be done by specialized personnel and is not very simple or user-friendly. Furthermore, initial settings can cause a loss of security and performance if made by non-specialists or inexperienced in cryptography.
2. It copies folders and subfolders to its "vault" - it does not encrypt the original folders and subfolders, which are then deleted.
3. The user/subscriber certificates are stored insecurely on the user's machine, encrypted with their password (c:\Users\<user>\AppData\Local\AxCrypt). They serve only to identify the subscriber.
4. This functionality must be enabled at the time of licensing. Companies can choose who will (or will not) have access to this functionality with maximum capillarity.
5. It does not allow the user to set a "secret key" per file but works with the access password used to authorize the application.
6. The user account password is required only upon opening the 1st file – after that, it is stored in memory, enabling anyone (or any program) to open protected files without requiring authentication.
7. Requires the "vault" opening key only.
8. AxCrypt shares files through RSA-4096-bit public keys automatically stored on your server. In addition, it stores the private keys for backup and synchronization between devices. Although the private key is encrypted with AxCrypt using the user-defined password, this usability feature can offer risks: 1) access to the product is enough to open shared files (no 2nd or 3rd security factors); 2) how to ensure that private certificates are not also stored unprotected?
9. Allows sharing of safe files by informing the access password, which creates risks. Does not allow sharing of encrypted partitions.
10. Allows encrypted file sharing without interaction with the manufacturer or third parties - for example, by using recipients' digital certificates and previously entered secret keys. In the case of BOXCRYPTOR, it stores all keys, both symmetric (AES) and asymmetric (Public and Private certificates).
11. OBAKE does not require additional files for sharing. Each authorized user’s data is inside the encrypted file. Without the proper recipient's private certificate, there is no risk of attacks and decryption.
12. Allows you to open the encrypted file in your associated program with just one click/ENTER, automatically re-encrypting it using the same parameters in the file (key or certificate) and in a transparent way to the user.
13. The vault must be open, exposing the contained files in a disk-virtual connection. However, as long as the vault is not manually closed, it will be available for access via Explorer or other programs using the same APIs.
14. Some programs require a folder (or an archive) to be created that will contain all the other protected files - thus the name "vault" - forcing the user to keep his files confined within this structure. The user’s files/folders structure is sacrificed…
15. Critical functions such as mandatory sharing, choice of algorithm, use of a secret key, sanitization, and others may be restricted to user modifications (CORPORATE version).
16. Access to critical settings is by pre-authorized personnel through login and 2-factor authentication. This authorization is given by a separate program, protected by a password and certificate exclusive to each company. In addition, all performed operations are informed to any previously authorized areas or people through a LOG issued by e-mail.
17. Only by password, which, if leaked, puts access to the environment at risk.

18. Copies can be "locked inside the code" to share any encrypted data between people or areas of the company (exclusively), with no quantity limit. The IT teams cannot delete such sharing (CORPORATE version).

19. Each area can authorize sharing information to predetermined people or areas through a restricted and secure configuration, ensuring high capillarity in this operation (CORPORATE version).

20. Restricted configurations, accessed only by authorized personnel (CORPORATE). See also topic 16.

21. Boxcryptor: all passwords, logins, and other authorizations are strings of HASHes based on the "password" informed by the user, giving a false sense of security. The attacker will not attack the HASH but the password created by the user (usually weak).

22. Offers the excellent 448-bit Blowfish, despite non-compliance with established standards.

23. OBAKE operates between 5 and 11 different keys (it depends on data size): 1 x 32 bits, 2 x 65536 bits, 1 to 4 x 512 bits, and 1 to 4 x 2048 bits.

24. Cryptographic keys independent of user input, aggregating random components and "one-way" calculations for reinforcing insecure keys.

25. Test on ten files: 1 RAR of 2.3 Gb, 2 DOCX of 3.5 Mb each, 1 XLSX of 10 Kb, 2 XLSX of 9 Kb each, 1 PDF of 1.2 Mb, 1 PDF of 58 Kb, 1 TXT of 100 Mb, 1 TXT of 1 kb. OBAKE was set to COMPRESS OFF and CHECK OFF to simulate the same operations as its competitors. Algorithms used: OBAKE and AES-NI. Times are purely illustrative and may vary depending on the hardware and programs running during the test.

26. In theory, the program uses and meets the mentioned standards, but using 56-bit keys, puts the effectiveness of the proposed cryptographic protection in check.

27. It does not accept the use of the Windows Certificates Store. Key storage can be on the server (encrypted by the HASH of the password) or in local mode - in which case the sharing process is sacrificed.

28. Provided if you share the key files (see topic 29) and use the Boxcryptor server (see topic 27).

29. All sharing is done through a "key file" that embeds the AES-symmetric key used in the file, encrypted with the public digital certificate of the recipient user. For example, if the file is shared with ten people, each person will have ten additional independent and relative files. All files are AES encrypted using the HASH of the user's password. A single encrypted file will have "N" key files directly proportional to the number of users authorized to view the file. See also topic 11.

30. A server required exclusively for File and Folder Sharing, Setup of a new Device, Data or Key Recovery, Group Creation/Edit/Delete, and Synchronization. Individual decryption or encryption does not require a server.

31. You can set up a MASTER-KEY for cases where the user(s) forget their password, from which all HASHes and protections are derived (see topics 28, 30). This MASTER-KEY recovery of the files encrypted by these users will only be possible if they are shared with others and available on the Boxcryptor server.

32. If the company has chosen the server environment with MASTER-KEY (see topic 31), the certificates and encrypted data can be recovered through a credential theft or "insider" attack.

33. Available in the CORPORATE version or as a separate module (PERSONAL).

34. Access protection for certificates, passwords, and keys follows the PBKDF2 standard with HMAC512 - a secure standard, but in this case, it will always be derived from the user's password.

35. Many programs use a "common key" for encrypting data for groups of users. OBAKE allows you to create groups where each individual will use his digital certificate so that each component of the group is subject to independent controls linked to each certificate (secrecy, availability, and revocation of the certificate). In addition, it translates into much better privacy than other group solutions.

36. These operations were conducted on the same computer sequentially. However, the RAM and cache were clean between each process.

37. The integration is performed by triangulation with the WHISPLY service, which can be commanded by the user or through the application. In this case, the user must inform the account data (login/password), so the program can transmit the files. On the other hand, OBAKE (and others) require no such data, working seamlessly in shared/synchronized folders.

38. The program requires a login/password and allows using a 4-character/number PIN. In this case, besides the PIN being of insufficient size, it does not rely on 2nd-factor authentication.

39. Only on the corporate version.

40. Additional libraries need to be obfuscated or adequately protected. The program is partially shielded, therefore.

41. Only through rules created on the Boxcryptor server or by sharing Active Directory rules.

42. The OBAKE encryption with digital certificate sharing embeds all authorization data within the encrypted files. This translates into more security, smaller size, and much less bureaucracy - the user is not required to share e-mail addresses or authorization files for each authorized person or group. In addition, we preserve a crucial feature: our encryption is genuinely "end-to-end"; nothing is transmitted or sent to any server, ensuring absolute user privacy from the moment a protected file is created.

43. AES-256-NI: fully compliant AES algorithm established within specific CPUs as of 2010. Performance rate easily triples the best ASM/C++ implementations.

44. OBAKE offers "ChaCha20-AEAD-Poly1305" (used by Google in its secure connections) and the "XSalsa-AEAD-Curve25519-Poly1305", more up-to-date and stronger version of the excellent algorithm used in TLS 1.3.

NAWKA CYBERSECURITY