Chapter 5
MKD (Memory Key Distribution)

MKD (Memory Key Distribution) takes a completely different approach to QKD and RKD, where cryptographic keys are generated and distributed from transmitted photons or radio signals. With MKD, non-deterministic random number generators generate the cryptographic keys, and the keys are transmitted using highly secure hardware tokens (usually ISO7816 smart cards) or special portable storage media (usually SSDs) with highly secure access protection for the data. Only highly secure storage media can be used for a one-time pad [WP–OTP][1] (sect 6.2) for subsequent data encryption and thus for cryptography that is entirely free of mathematics (except for XOR).

5.1 Precursors to MKD

The history of MKD (Memory Key Distribution) began around 2500 years ago. At that time, encryption was carried out using the Scytale (staff) of Sparta [WP–Scy].[2] In the early days, the keys were usually transported by envoys, diplomatic couriers, messengers, priests, or soldiers, and their brains were usually the "memory." Later, paper, teletype paper tape, microfilm, film strips, etc. were mostly used. With the advent of electronic storage media, magnetic tapes, cassettes, CDs, etc. were also used. Steganographic methods [WP–Ste],[3] glued nut shells (Fig. 5.1), private folds (letter locking), sealed envelopes, personal diplomatic bags, sealed capsules, secure containers, and even armored suitcases (sometimes with self-destruction devices) etc. were often used for hiding. Special hardware-based encryption boxes were usually used for encryption.

[1] https://en.wikipedia.org/wiki/One-time_pad.

[2] https://en.wikipedia.org/wiki/Scytale.

[3] https://en.wikipedia.org/wiki/steganography.

E. Piller and H. Schölnast, *Data Encryption at the Intersection of Mathematics and Physics*, SpringerBriefs in Information Security and Cryptography,
https://doi.org/10.1007/978-3-032-24764-3_5

Fig. 5.1 A precursor to MKD

Storage media with their own high-security access protection did not come onto the market until the 1980s, with the introduction of high-security smart cards with processors [Rankl10][4] in accordance with ISO/IEC 7816 [WP–Iso],[5] as used in passports and payment transactions. However, due to their low storage capacity, they are only suitable for subsequent mathematical encryption methods. At that time, data encryption was usually carried out using the DES method or Triple DES [WP–3D].[6] Today, AES-256 [WP-AES][7] is mostly used for this purpose. In the high-security area, encryption is usually carried out in an HSM (Hardware Security Module [WP–HSM][8]; see https://cryptography.study/phys/HSM). MKD with smart cards for key exchange and a mathematical method for data encryption is very interesting today and will continue to be so in the future if mathematical methods are accepted. Because this is usually the case today, MKD with smart cards and mathematical encryption is also the most widely used variant in practice.

Cost-effective portable storage media with highly secure access protection and internal data encryption for the use of a one-time pad [[Rij22],[9] Bell11,[10] [Bor12][11]] are achievements of this century. In this book, which deals with physical methods and, for security reasons, includes all cryptographic security objectives, i.e., data encryption for confidentiality, MKD prefers MKD-capable portable storage media with sufficient storage capacity for one-time pads.

It was not until 1976 that the first mathematical method for generating and distributing cryptographic keys over insecure channels was published by Diffie and Hellman [[WP–DH],[12] [Diff22][13]], which is now also available in quantum

[4] https://www.wiley.com/en-us/Smart+Card+Handbook%2C+4th+Edition-p-9780470743676.

[5] https://en.wikipedia.org/wiki/ISO/IEC_7816.

[6] https://en.wikipedia.org/wiki/Triple_DES.

[7] https://en.wikipedia.org/wiki/Advanced_Encryption_Standard.

[8] https://en.wikipedia.org/wiki/Hardware_security_module.

[9] https://ciphermachinesandcryptology.com/papers/one_time_pad.pdf.

[10] doi:10.1080/01611194.2011.583711.

[11] https://ieeexplore.ieee.org/abstract/document/6387923.

[12] https://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange.

[13] doi:10.1145/3549993.3550007.

computer-secure variants. Due to the logistical effort required for the physical distribution of keys, MKD, i.e., the purely physical distribution of cryptographic keys, continued to lose importance. In particular, MKD became completely uninteresting in the mass market. Mathematical methods in the form of asymmetric cryptography have revolutionized cryptography, but the generation and distribution of keys using physical methods remain relevant where very high data security is required.

5.2 MKD

As mentioned above, MKD can use highly secure smart cards, such as those used today in payment cards, passports, etc., to generate and distribute cryptographic keys. However, the low storage capacity is only sufficient for data encryption using a mathematical method such as AES-256, which is sufficient for most applications today. This also applies to key exchange with an HSM or asymmetric key exchange in conjunction with a pre-shared key (PSK) in a stationary HSM.

In the following, MKD in conjunction with a one-time pad is preferred for encryption because this is the only way to ensure absolute data security throughout, from key generation and key exchange to the cryptographic security goals of confidentiality and integrity of the data.

This MKD with a one-time pad consists of at least two required devices and several process steps. The devices are MKD-capable portable storage media and non-deterministic random number generators. For security reasons, highly secure smart cards are usually used in addition, which contain a PIN (Personal Identification Number [WP–PIN][14]) for accessing the smart card and the keys used to encrypt the key bits on the storage media. The components required for MKD with a one-time pad, such as MKD-enabled storage media, random number generators, and smart cards, are available as mass-produced goods on the global market. This has a very positive effect on price, global availability, deliverability, maintenance, service, manufacturer change, supplier change, compatibility, and security assessments.

5.2.1 MKD-Capable Portable Storage Media

MKD-compatible portable storage media (Fig. 5.2) consist of at least six important components and requirements in terms of security technology:

1. Storage medium, currently implemented as a memory stick, SSD (solid state disk), or NVMe SSD (non-volatile memory express SSD). NVMe SSDs are characterized by particularly high read/write speeds, currently up to approx.

[14] https://en.wikipedia.org/wiki/Personal_identification_number.

Fig. 5.2 MKD-compatible portable storage medium

7 GB/sec. Memory sticks are currently available on the market with capacities of up to 256 GB, SSDs and NVMe SSDs with capacities of up to 16 TBytes.

2. PIN input device for PIN entry directly on the storage medium. A PIN change is only possible after entering the correct PIN. PIN checks can be performed on the external smart card and/or in the storage medium. Solutions where only a PIN check is performed in the storage medium and no smart cards are required are not recommended. There are also providers offering fingerprint recognition.
3. Smart card reader in accordance with ISO 7816. This reader is used to transfer the PIN entered on the storage medium to the smart card and to transfer the key from the smart card to the integrated AES-256 HW encryption unit via the smart card reader.
4. Integrated AES-256 HW encryption unit. All key bits sent from outside for storage in the storage medium are encrypted by the HW encryption unit and are decrypted again when read. In the better products, the encryption/decryption key comes from the external smart card, but it can also be stored in the storage medium. However, the smart card solution is more secure because it operates

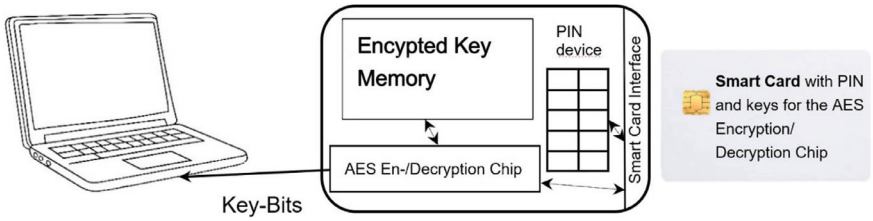

Fig. 5.3 Activation of a secure storage medium with PIN and smart card

Fig. 5.4 Laptop with TRNG (true random number generator) and an MKD-compatible portable storage medium with a smart card

separately from the storage medium and therefore the encryption/decryption key is always missing in the event of a physical attack on the storage medium.
5. Certifications.
6. SATA or USB interface to the outside for data transfer.

Most products available on the market are also water-, dust-, and shock-resistant. This means they can also be used in harsher environments and, with security restrictions, can be transported using public service providers.

In addition to the storage media, high-security smart cards with processors in accordance with ISO/IEC 7816 [Rankl10][15] are required. The keys for encrypting/decrypting the data on the storage media are generated on these smart cards, and the keys are PIN-protected with an error counter (e.g., 3 attempts); see Fig. 5.3. Figure 5.4 shows a laptop with a random number generator and MKD-enabled storage media.

If the number of failed attempts is exceeded, the keys are no longer accessible. When the correct PIN is entered, the keys are transferred to the storage medium and used there to encrypt/decrypt the stored key bits by the internal AES HW encryption unit. Usually, two smart cards are used for one storage medium. There are also high-security SSDs and NVMe SSDs without these smart cards. In these, the key for AES

[15] https://en.wikipedia.org/wiki/ISO/IEC_7816

HW encryption is stored internally in the encryption unit. This variant offers lower security and should therefore be avoided with MKD. There are also MKD-enabled SSDs that contain additional protection mechanisms, such as zeroization [WP–Zer][16] (self-erasure in the event of an attack attempt).

Additional components and functions are possible. The components include, for example, sufficiently fast integrated non-deterministic random number generators, which are still far too slow in the current market offerings. HSMs are only necessary for telecommunications applications in conjunction with PCs (e.g., laptops), servers, etc., and MKD with a one-time pad if the PC is not protected.

In practical application, each user must have an MKD-capable portable storage medium on site where the data is encrypted/decrypted, e.g., on a desktop PC, laptop, etc., with/without an HSM. Another MKD-enabled portable storage medium is used for key transport. For telecommunications applications, each user requires an MKD-enabled portable storage medium and a non-deterministic random number generator. For data storage applications, only role administrators require a non-deterministic random number generator and multiple MKD-enabled storage media.

If key distribution (transport of storage media) takes place in person between communication partners or between role managers and role-access-authorized persons, the logistics are relatively simple. However, with multiple system participants, this transport of keys becomes complex and is usually carried out with the help of third parties. This requires additional tasks in the logistics process. A documented chain of custody (chronological documentation of evidence [WP–COC][17]), expanded with additional necessary tasks, serves as a model for this. A chain of custody comes from the legal field and describes the secure and traceable process from the identification of evidence, e.g., by the police, to its presentation in court. Details on the logistics of secure key transport are provided in Chapt 7.3, which covers topics and aspects such as typical procedures, documented chain of custody for MKD processes, process steps, sender and recipient authentication, confirmation of receipt, recall mechanisms, documentation requirements, and technological support for the logistics process.

5.2.2 TCG Opal Standard

In addition to the above requirements for MKD-enabled storage media, there is also an international standard that describes how MKD can be applied with a one-time pad. It is called TCG Opal [[WP–Opa],[18] [TCGOpa][19]]. TCG stands for Trusted

[16] https://en.wikipedia.org/wiki/Zeroisation

[17] https://en.wikipedia.org/wiki/Chain_of_custody.

[18] https://en.wikipedia.org/wiki/Opal_Storage_Specification.

[19] https://trustedcomputinggroup.org/resource/storage-work-group-storage-security-subsystem-class-opal/.

Computing Group [WP–TCG],[20] which develops open, vendor-neutral, industry-standard specifications for trusted computer components and software interfaces on multiple platforms, and is operated by leading companies in the computer industry. Opal was developed to increase the security of storage media and is designed to make hardware encryption integrated into storage media simple and secure. The storage media are called Opal SEDs (self-encrypting drives). SEDs are self-encrypting drives based on hardware encryption (usually AES-128 or AES-256). MKD-enabled storage media that comply with TCG Opal SSC specifications have the following features relevant to MKD with a one-time pad:

- The encryption of data—in the case of MKD, the key bits—is always performed by hardware on the storage medium itself. According to Opal, the key for this hardware encryption is also stored on the storage medium. Some of the storage media suitable for MKD allow this key to be stored externally on a smart card, and the key is not stored on the storage medium (only used during encryption/decryption). This extension of Opal is strongly recommended for MKD with a one-time pad.
- SEDs based on Opal 2.0 implement extended key management via both an authentication key (AK) and a second-level data encryption key (DEK). Key management takes place within the disk controller chip.
- Since encryption is always active, the controller automatically decrypts the contents of the permanent memory during the read process. If greater security is desired, an additional ATA password can be set. However, if this password is lost, it is no longer possible to read the stored data—in the case of MKD, the key bits— which is not a problem for MKD with a one-time pad in telecommunications applications, but it is a problem for data storage applications.
- Opal enables sector-specific authorizations with separate access rights. Each area can be created, edited, and deleted independently. In telecommunications applications, this allows different communication partners to be separated, and in data storage applications, different roles (each role has its own keys). This highly secure separation offers major security advantages for MKD, especially the separation between telecommunications and data storage.

5.2.3 Security Certification According to CC (Common Criteria) and EUCC

For security certifications according to CC[21] and EUCC,[22] there are also CC profiles, e.g., BSI-CC-PP-0081-2012, Portable Storage Media Protection Profile (PSMPP), Version 1.0 [BSI12].[23]

[20] https://en.wikipedia.org/wiki/Trusted_Computing_Group.

[21] https://www.commoncriteriaportal.org/index.cfm.

[22] https://certification.enisa.europa.eu/certification-library/eucc-certification-scheme_en1.

[23] https://www.commoncriteriaportal.org/files/ppfiles/pp0081b_pdf.pdf.

The TOE (Target of Evaluation) described in this protection profile is a portable, self-contained storage medium such as a USB stick or a portable SSD with a physical connection for a computer. It offers encrypted storage of user data (in the case of MKD, these are the key bits) and strong authentication to grant access to the encrypted data. This protection profile for mobile data carriers is divided into a "basic" part and an (optional) "extended package part." An extended package allows flexible adaptation to specific requirements, such as stronger authentication functionality, without having to completely revise the protection profile. The evaluation is carried out for two variants of the PP: for the basic part and for the extended package part. The data in the protected storage area of the portable storage medium must not be accessible to unauthorized persons if the medium is lost, misplaced, or stolen. To this end, the protection profile defines a basic set of security requirements to cryptographically ensure the confidentiality of the data in the protected storage area against logical or physical attacks. The default power-up state of the device only provides access to the authentication mechanism. An essential aspect of IT security is that the security functions are implemented entirely within the storage medium. Overall, the EVG implements the following important security features:

- Protection of the confidentiality of user data— in the case of MKD, the key bits for telecommunications and data storage applications— through encryption.
- Protection of TSF data (authentication data, internal encryption keys, etc.).

5.2.4 Non-deterministic Random Number Generators

Non-deterministic random number generators [[Vai23],[24] [John18][25]] use physical processes such as thermal noise, radioactive decay, or quantum-optical processes [[Meij19][26]] to generate random numbers. They provide truly random numbers (bit sequences) that represent non-reproducible number sequences (bit sequences). However, they are slower than deterministic generators because they rely on real physical processes. It is very important that at least two separate random number generators are always used, if possible from different manufacturers. This ensures that even a faulty or poor random number generator—possibly caused by an attacker or the manufacturer—cannot pose a security problem, because after an XOR operation on the generated key bits (random numbers), the better of the two generators always determines the minimum quality of the key bits. This is standard practice in MKD, but it also applies to QKD. Details on non-deterministic random number generators, including a current market overview, are available on the book's website at.[27]

[24] doi:10.1007/s11128-023-04175-y.

[25] doi:10.1515/9781501506062.

[26] doi:10.1109/SP.2019.00088.

[27] https://cryptography.study/phys/TRNG.

5.3 Process Steps for MKD

When it comes to the process steps of MKD with a one-time pad, a distinction must be made between telecommunications and data storage applications.

5.3.1 Telecommunications with MKD Using a One-Time Pad

In the field of telecommunications, two of these MKD-capable portable storage media are used on both sides (communication partners A and B). One of these is used for encrypting and decrypting the data on site (at A and B)—this storage medium is therefore called the encryption/decryption storage medium—and the second storage medium is used for key transport—this storage medium is called the transport storage medium. The transport storage medium has a size of 512 GB, for example, and the encryption/decryption storage medium has a size of 16 TBytes. This allows the key bits for telecommunications with 32 different communication partners to be stored on site.

In addition, highly secure smart cards in accordance with ISO-7816 with processors are used. Usually two per communication partner A and B are used.

Both communication partners A and B also require a non-deterministic random number generator to generate the necessary key bits (Fig. 5.5).

Process Steps

In the first process step, a smart card on both sides (communication partners A and B) generates a key for AES HW encryption in the portable storage medium and receives a start PIN. This key is then copied to a second smart card, which also receives a start PIN. To avoid copying the key to the second smart card, this process can also be carried out using a Diffie-Hellman key exchange procedure, which generates the key for AES HW encryption in both smart cards simultaneously and separately.

In the second process step, a random bit sequence (called S_A and S_B) is generated on both sides (communication partners A and B) using a non-deterministic random number generator, which is stored on each side (A and B) on a transport storage medium and on its own encryption/decryption storage medium (Fig. 5.5). During this storage process, the bit sequence is automatically encrypted in the storage medium itself using the smart card key before the storage process (process step 1).

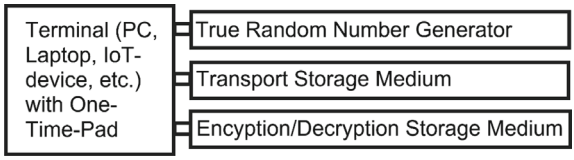

Fig. 5.5 MKD during key generation

In the third process step, each of the two transport storage media and one of the two smart cards are transported to the other side (from A to B and from B to A) in person, by a trusted courier, or by a public parcel service. When using a public parcel service, the storage medium and smart card must be transported separately, which is always advisable. The smart card can also be transported only once at the very beginning, before the first transport of the transport storage medium. Over time, e.g., annually, the smart card can be renewed, which again results in transport.

In the fourth process step, the key bits received by the transport storage medium are then stored on both sides—after internal decryption by the AES HW encryption unit with the smart card key—in the own encryption/decryption storage medium under the name of the sender. This means that the encryption/decryption storage medium on both sides A and B then contains the key bits S_A and S_B in two different files—the file name is always the name of the generator of the key bits.

These key bits are then used on both sides in the fifth process step for encrypting/decrypting the data (see Fig. 5.6). Communication partner A uses the key bits from file "A" for encryption, i.e.,S_A, and communication partner B uses the key bits from file "B," i.e.,S_B. It follows that the sender's key file is always used to encrypt and decrypt the transmitted data. This means that both communication partners can always use new key bits for encryption and no key bits are used multiple times, even though there is no synchronization between the two communication partners. The sender from whom the data to be transmitted originates is always responsible for the quality of the key used.

In a second variant of this key exchange, both communication partners do not use their own key bits for encryption, but rather the key bits are created by an XOR link between both communication partners, i.e., A and B jointly generate the key bits for both communication directions. In the second process step of this variant, two random bit sequences for the key bits are generated on both sides (A and B) with the aid of a non-deterministic random number generator, i.e., on side A, S_{A1} and S_{A2} are generated, and on side B, S_{B1} and S_{B2} are generated, which are stored on each side (A and B) on a transport storage medium and on their own encryption/decryption storage medium. After transport, in the fourth process step, the key bits received by the transport storage medium are stored on both sides in the encryption/decryption storage medium under the name of the sender on side A in the form S_{A1} XOR S_{B1} and on side B in the form S_{A2} XOR S_{B2}. This means that the encryption/decryption storage medium then contains the XOR-linked key bits of both communication partners A and B in two different files—the file name is A for S_{A1} XOR S_{B1} and B for S_{A2} XOR S_{B2}. In this second variant, both communication partners can determine the quality of the key bits for both communication directions.

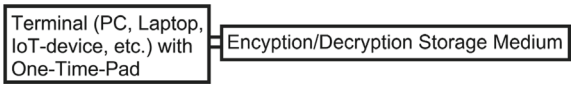

Fig. 5.6 MKD at the terminal device for telecommunications and data storage

In this environment, MKD is ideally suited for generating, storing, and exchanging keys using exclusively physical methods and for subsequent high-security data encryption with a one-time pad. Data integrity can be guaranteed with a MAC (GCM, CCM, CBC, etc.; see sect 2.6.2), which, like the one-time pad, also operates with the XOR function. The GCM-MAC and CCM-MAC also contain authentication data. Furthermore, the authentication of both sides A and B is perfectly solved by the transport of the smart card, and possibly also the storage media. Even when transporting the transport storage media via public parcel services, access protection to the transport storage medium with PIN and smart card provides a highly secure solution. From a security perspective, it must be taken into account that the encryption of the key bits for the one-time pad is performed with AES-256, i.e., with a mathematical procedure. If this encryption, including the certified access protection to the transport storage media, is classified as insufficiently secure, the transport of the transport storage media must be carried out personally or by confidential third parties. This closes the last non-purely physical gap, and MKD with a one-time pad can be classified as mathematically secure (except for the XOR function), even though it contains a mathematical procedure with AES-256 within the storage media, which only provides additional protection.

MKD can be integrated very well into telecommunications protocols.

5.3.2 Data Storage with MKD with a One-Time Pad

There are many possible solutions for highly secure data storage. Basically, these always involve an access control system based on physical cryptography, where read protection is ensured by encryption with a one-time pad. Below is an example of a solution that is easy to implement in practice and uses exclusively physical cryptographic methods. It is based on an authorization concept with roles, i.e., role-based access control [WP–RBA].[28]

In this solution, each user employs an MKD-enabled portable storage medium. This is used for encrypting and decrypting data on site at the user's location with a one-time pad and is therefore referred to as an encryption/decryption storage medium, as in the case of telecommunications above. A second storage medium, which is only used by role administrators, is used for key transport and is therefore called a transport storage medium. The transport storage medium has a size of 512 GB, for example, and the encryption/decryption storage medium has a size of 16 TBytes. If the key bits for data storage from 16 different roles are then stored on site, half of the storage remains available for the extension of role keys (see below).

A solution variant is presented below as an example.

Figures 5.5 and 5.6, "MKD during key generation" and "MKD at the terminal device during telecommunications and data storage," are also applicable here.

[28] https://en.wikipedia.org/wiki/Role-based_access_control.

Process Steps

In this role-based solution, the central function of key generation is performed by a role administrator, but it can also be a central office, etc.

In the first process step, the role administrator instructs a smart card to generate a key for AES HW encryption, and it receives a start PIN from the role administrator. This key is then copied to a second smart card, which also receives a start PIN. To avoid copying the key to the second smart card, this process can also be carried out using a Diffie-Hellman key exchange procedure, which generates the key for AES HW encryption on both smart cards simultaneously and separately.

In the second process step, a non-deterministic random number generator generates a random bit sequence of sufficient length (e.g., 512 GB).

In the third process step, the role administrator copies the random bit sequence from process step 2 to several transport storage media, depending on the number of subjects (read/write-authorized persons) of the role.

In the fourth step of the process, each subject of the role (authorized person, etc.) receives one of these transport storage media and one of the two smart cards from step 1, either in person or via a trusted courier. When using a public parcel service, the storage medium and smart card must be transported separately, which is always advisable. The smart card can also be transported only once at the very beginning, before the first transport of the transport storage medium. Over time, e.g., annually, the smart card can be renewed, which again results in a transport.

In the fifth process step, each subject then reads the key bits from the transport storage medium after decryption by the AES HW encryption unit using the smart card key. Each subject then copies the key bits as a file (called a role file) with the name of the role, a sequence number, and a generation number to its encryption/decryption storage medium. This means that the encryption/decryption storage medium then contains a roll file with the roll name and a sequence and generation number for all rolls to which the subject has access rights (read/write rights), which contains the key bits for this roll. Because new key bits are required for each storage of new data for the necessary encryption of this data (the one-time pad prohibits multiple use of key bits), all key bits of a role may eventually be used up (however, with the specified encryption modes, this only applies to one mode; see Sect. 6.4.3). The role administrator must then deliver a new file with key bits using the transport storage medium. This new file has the same name (the name of the role) and the same generation number, but the sequence number is increased by one. This allows the key bits of a role to be extended. Because all key bits ever used for data encryption are required again during a read operation as long as the encrypted data is still in use, and because years may elapse between the write operation (including data encryption) and subsequent read operations (including decryption), these key bits must be stored locally in the encryption/decryption storage medium for a correspondingly long period of time.

When a user (subject) leaves a role, new key material must be used for all future encryptions, i.e., process steps 2 to 5 must be repeated. In this case, a role administrator must send a new key file to all remaining users (subjects) of a role. This invalidates the unused key bits, and the user who has left the role can no longer use

them. However, before the sixth process step can be performed, a pause is required until all users in the role have received the new key bits. This pause can last a few hours, but also several days if the transport is over a long distance. During this pause, the old key bits are still valid. The user who has left the role can still read the data for which they still have the key bits. However, this is not a disadvantage, as they also had free access to this data before leaving the role. In the fifth process step, each user (subject) remaining in the role reads the new key bits from the transport storage medium. Each user (subject) then copies the key bits as a role file with the name of the role, a sequence number, and a generation number to their encryption/decryption storage medium, whereby the generation number is increased by one.

In the sixth process step, these key bits of the roll file are used for encrypting/decrypting the data. Sect 6.4 and https://cryptography.study/phys/modes presents four different encryption methods/modes for encrypting/decrypting the data, three of which are methods/modes newly developed specifically for QKD and RKD. The methods/modes, called OTPH, OTPS and XTSO, do not require any additional key bits for each subsequent encryption of data blocks, i.e., the key length for the one-time pad is constant (Key1 plus Key2 plus Key3) plus a special counter (Chap 6.4). These encryption methods/modes do not require a mechanism for extending the role file, i.e., the sequence number loses its meaning, but the generation number must be retained because when a user (subject) leaves a role, the role key (Key1, Key2, and Key3) must be changed. This means that when a subject leaves a role, the same amount of new key material, including the counter, is required, and the key bits, including the file, are stored in the role file with the name of the role and a generation number increased by one.

If the application requires the key to be generated from several different key bits, several role administrators can generate key bits separately and use an XOR operation to determine the final key, which is then stored on transport storage media for all subjects.

Since the sequence number of a key file becomes larger and larger over the years, but much of the stored data is no longer used because it has already been deleted or replaced by new data, for example, for efficiency reasons, the sequence number can be restarted from the beginning by re-encrypting the data that is still relevant, and all old key bits of the file can be deleted. This applies to all three specified encryption methods/modes.

A problem with the data storage application can occur in networks when several users modify and thereby encrypt data in the same file or database at roughly the same time. This can lead to synchronization errors, which are not possible in the telecommunications application because each user uses their own key bits. However, if handled correctly, these synchronization errors do not have to lead to any errors. In encryption mode 3 (one-time pad), they can lead to individual key bits being used multiple times in exceptional cases. This problem can only be solved perfectly if, as in telecommunications, each user uses their own key bits and a role administrator no longer generates and distributes them to all subjects. However, this leads to a significantly larger number of role files, because each role file contains not only

the sequence and generation number but also the user name and must therefore be available more often.

5.4 Summary

With MKD for one-time pads, the physical generation and distribution of cryptographic keys can be implemented with a high level of security. This is supported by the extremely high data volume, currently up to 16 TBytes for a single transport, which takes a few hours to days, key rates currently up to 7 GB/sec, high robustness in terms of temperature, shocks, etc., extensive certifications, access protection to the key bits with PIN and smart card, extensive standardization (USB, SATA), unrestricted suitability for mobile end devices, and, above all, the low price (currently $1100 for 1 TB with smart cards, $3000 for 16 TB). In addition, there is the required non-deterministic random number generator, currently costing around $1100 for fast key generation based on quantum-optical processes; slower non-deterministic random number generators are currently available from $65.

There is currently a wide range of MKD-enabled portable storage media on the market that are used today as portable storage media for high-security data backup, but which are also suitable for MKD. More information about such storage media can be found on the book's website at.[29]

These features of MKD with a one-time pad and easy usability with today's end devices via the USB or SATA interface—with or without connection to an HSM—allow highly secure end-to-end encryption in telecommunications and on-site data storage (on a PC, etc.) with a one-time pad, even with common end devices such as PCs, laptops, etc. Data encryption can then be performed in an HSM or directly on the PC.

MKD with a one-time pad also allows use in mobile devices for telecommunications and on-site data storage, thanks to the portable storage medium for all required key bits. This means that on a laptop—with or without a connection to an HSM—cryptography based entirely on physical processes (key generation and distribution, data encryption/decryption, MAC calculation, data authentication) can be implemented for seamless, highly secure data security, even during a train journey, flight, etc. The security requirements always lie with the end device and the MKD-enabled storage medium. This also applies to mobile IT systems in locomotives, cars, ships, weapon systems, etc.

With a 1 TB (1 TByte) MKD-compatible storage medium, telecommunications can be encrypted with a one-time pad for a long period of time with provable 100% security. The background software is very simple, as is the synchronization between the two communication partners (each partner uses only its own key bits for encryption). Decryption by an attacker on the communication link is completely impossible today and in the future, even for intelligence services. The "data storage" solution is

[29] https://cryptography.study/phys/memory.

more complex (see above). The "data storage" solution is more complex. However, the LISA solution (see Sect. 7.1.1), which was used for the MKD- tests, shows that data storage in a PC environment (even without the use of an HSM) can also be highly secure and function perfectly.

5.5 Counterarguments to MKD

Considering Memory Key Distribution (MKD) as a method for generating and distributing cryptographic keys requires explicit consideration of objections that arise less from the cryptographic idea and the physical possibilities themselves than from questions of scaling, organizational embedding, logistical processes, and legal framework conditions. These aspects relate to the implementation level and have a decisive influence on how MKD can be handled in practice in larger structures.

- **Scalability.** As with all methods involving paired-shared secrets, the organizational effort increases quadratically with the number of communication partners involved. For n participants, this results in a requirement for $n \cdot (n-1)/2$ independent key relationships in the worst case. This n^2 dependency is also found in the same form in QKD and RKD systems, which in the case of QKD is counteracted by KMS networks with trusted nodes, but this increases the attack surface. With MKD, this problem only affects the upstream key provisioning. With MKD, ongoing operation is not limited by continuous key rates (as with QKD and RKD), but by the one-time provisioning of sufficiently large key material. Scaling thus becomes an organizational issue (see Sect. 7.3) rather than a physical-technical limitation.
- **Logistical and Procedural Risks.** Such risks must be taken into account, particularly in connection with the physical transport of storage media. Possible vulnerabilities include interruptions in the documented chain of custody, loss, theft, or improper handling of data carriers. These risks are real and inherent, but differ fundamentally from attack vectors in transmission-based methods such as QKD and RKD. However, risks in MKD are concentrated in clearly definable process steps. The security-critical period is limited in time and space. This makes risks easily visible, verifiable, and addressable at the organizational level.
- **Organizational Fault Tolerance.** The effectiveness of MKD depends on clearly defined responsibilities, clean documentation, and disciplined process execution (see also Sect. 7.3). Human error or organizational oversights can compromise security. However, this dependency is not unique to MKD, but characterizes all high-security procedures whose protective effect is not exclusively enforced by technical means. In contrast to complex, continuously operated technical systems, deviations from defined processes in MKD do not lead to creeping security losses over long periods of time. Errors take effect immediately and force a clear response, such as the reevaluation or replacement of key material.

- **Regulatory and Liability Issues** relating to MKD primarily concern the handling of physical data carriers, personal access devices, and transport services. In many jurisdictions, there are established regulations for this from related areas such as confidentiality, data carrier classification, or high-security logistics. MKD thus operates within known regulatory patterns instead of opening up new, technically elusive problem areas. Liability issues can be clarified on the basis of specific process responsibilities. Security-related events are linked to physical actions, times, and responsibilities and are therefore fundamentally traceable. This differs from scenarios in which security breaches can only be identified retrospectively and without a clear analysis of the causes.

These counterarguments show that the challenges of MKD do not lie at the level of cryptographic security, but rather in scaling, organization, and logistical implementation. These challenges are clearly identifiable, analytically accessible, and not obscured by idealized assumptions about technical components or transmission channels. MKD thus deliberately shifts security-related issues into an area that is characterized by processes, responsibilities, and control and differs fundamentally from transmission-based physical processes.

5.6 Security Considerations

Portable MKD-enabled storage media for small amounts of data, where mathematical cryptographic methods are subsequently used, are primarily high-security smart cards with processors in accordance with ISO/IEC 7816, as used in passports, SIM cards, and payment transactions [Rankl10]. They are all available with high-security certifications (CC EAL4+) in various designs, such as cards, USB sticks, wristbands, chips, etc.

Portable storage media available for MKD with a one-time pad[30] contain at least one access protection, integrated AES HW encryption, a PIN input device, smart cards, etc., are security certified and are currently available up to 16 TB. Additional security features are available in some cases. When transporting storage media personally or through a trusted third party, the transport route and, above all, the very important authentication of the partners are additionally secured.

The number of security-critical components and the security of each of these components are also interesting from a security perspective, because no manufacturer develops and produces all of these components themselves (for details, see Sect. 7.2).

In contrast to QKD, MKD with a one-time pad contains only a few security-critical components. At the highest level, this involves the non-deterministic random number generator and at the lower levels access protection for the storage medium with the necessary components. This also applies to side-channel attacks, which represent a wide field of activity for attackers in QKD and RKD and are difficult to assess

[30] https://cryptography.study/phys/memory.

completely due to their high complexity in some cases. With MKD using a one-time pad, side-channel attacks are easy to understand and assess due to their simplicity. Side-channel attacks via measurement of radiation and power consumption are only possible during operation and only immediately next to the device. If the storage medium remains switched on or in standby mode after operation and the internal AES key is still in the RAM, an attacker could read the RAM by physically cooling it down. However, this is hardly feasible in practice because the RAM is protected in the AES chip and the AES chip is built into the storage medium.

When transported personally or by a trusted third party, the device is never in an operational state and therefore there is no radiation or power consumption and no possibility of reading the RAM, and the storage medium is always under control.

Transportation by a public service provider allows for an attack scenario that requires a great deal of effort, leads to the destruction of the storage medium, but then fails at the level of AES encryption in the storage medium because the encryption key is stored on another storage medium (the smart card) (hence the requirement for a smart card for key transport for AES HW encryption). However, if the AES encryption itself becomes a successful attack scenario because it is a mathematical encryption method, MKD must be transported personally or by a trusted third party, because this transport also reliably prevents this attack scenario.

However, the central security component of an MKD solution is the non-deterministic random number generator. Particular attention must be paid to the quality of the random numbers, because the random numbers determine the quality of the key and thus the data encryption. Because key quality is very difficult to verify, high-security certifications are particularly important here. The environment, i.e., the supplier, etc., should also be checked (see Sect.7.2) and several different random number generators should be used.

5.7 Practical Criteria

5.7.1 Market Readiness

Suitable portable storage media for MKD[31] with one-time pads and non-deterministic random number generators are already widely available on the market.[32] A suitable complete software solution for data storage with and without HSM is also available on the market (see Sect.7.1.1). Integration into web browsers is not known for MKD with one-time pads, although it is easy to implement.

[31] https://cryptography.study/phys/memory.

[32] https://cryptography.study/phys/TRNG.

5.7.2 Key Rates

Key rates depend on the read speed. For MKD-enabled NVMe SSDs, they are currently around 7 GB (GBytes) per second. This key rate is well above the key rates of QKD and RKD and can be guaranteed for MKD throughout.

This does not take into account the generation of the key bits. To "fill" a 1 TB storage medium with non-deterministic random numbers, very fast non-deterministic random number generators that use quantum-optical processes (240 Mbit/sec, price approx. $3600) are required, which take around 9 hours. Non-deterministic random number generators with a USB interface, which also use quantum-optical processes and are in the price range of around $1100, only deliver slightly more than 4 Mbit/sec, which requires around 23 days for a 1 TB storage medium. Slow random number generators usually require an upgrade to a hybrid generator to reduce the time required, i.e., additional numbers are calculated from the non-deterministic numbers using a suitable algorithm so that the rate can be increased, for example, 20fold. However, this reduces data security, which may be relevant.

5.7.3 Distance of Key Transmission

The distance only affects the duration of transport of the portable storage medium and ranges from a few hours to several days. This means that with MKD using a one-time pad, up to 16 TB of random key material can currently be exchanged nationally and worldwide in a few hours to days in a highly secure manner between "n" participating partners/end devices. With MKD, the destination address can change regularly because the storage medium is physically transported, which requires extensive preparation and costs with QKD.

5.7.4 Cost Framework

The cost of MKD-enabled portable storage media currently ranges from approximately $1,100 for 1 TB with smart cards to $3,000 for 16 TB (see the book's website at[33]). For HSMs, the cost is approximately $1600 for the PC solution (see the book's website at[34]). In addition, there is the required non-deterministic random number generator, which costs from around $1,100 and, in some applications or application environments, can be provided by trusted central units and can therefore be more expensive and thus faster. Fast non-deterministic random number generators

[33] https://cryptography.study/phys/memory.

[34] https://cryptography.study/phys/HSM.

that operate on the basis of quantum-optical processes cost from $1100, and around $3,600 for very high bit rates (see the book's website at[35]).

During operation, the costs of transporting the storage media must also be taken into account. For public service providers, this amounts to only a few dollars per transport, and for transport with confidential third parties or personally over short distances, the costs are low, but for long distances, higher costs (time and travel expenses) may be incurred. With distribution of storage media, e.g., to company locations, all storage media at a location can be transported at the same time, thus saving on higher costs.

5.7.5 Compatibility (with Today's Technology, Interchangeability).

Because the available portable MKD-enabled storage media have a USB interface in the case of memory sticks and usually a SATA interface in the case of SSDs (SSDs with USB interfaces are also available), they can be plugged directly into any PC, laptop, HSM, etc., and the stored cryptographic keys can be read directly. The non-deterministic random number generators currently contain a USB interface with a bit rate of up to 4 Mbit/sec and a standardized PCIe interface above that.

MKD-enabled storage media and non-deterministic random number generators are mass-produced goods on the global market and can therefore be easily replaced by other models or manufacturers/suppliers.

5.7.6 Robustness/Susceptibility to Interference

Portable storage media are very robust against temperature fluctuations, shocks, moisture, etc., because SSDs and memory sticks do not contain any mechanical components. MKD with a one-time pad therefore does not require any maintenance of the devices, which is always security-sensitive and involves extensive attack scenarios. If a portable storage medium breaks down, it can be easily and inexpensively replaced with a new one. Compatibility makes it easy to switch manufacturers, thus preventing delivery problems in the event of a supplier bottleneck.

[35] https://cryptography.study/phys/TRNG.

5.7.7 Suitability for Mobile Devices

Because portable storage media are very robust and relatively small and draw their power from PCs, laptops, HSMs, etc., they can also be used without any speed restrictions in mobile devices. This means that they can also be used without restriction in cars, rail vehicles, aircraft, ships, drones, etc. MKD with a one-time pad is therefore also suitable for telecommunications to and from aircraft (passengers or crew members), where highly sensitive/secret data is exchanged.

5.7.8 Randomness of the Keys.

The non-deterministic random number generator determines the randomness of the key on both sides when used for telecommunications. When generating the key, the sender of the data or both communication partners can equally determine the quality of the encryption, which leads to equality between both communication partners, which is often not the case with QKD.

In the data storage application, one or more role administrators take responsibility for the randomness of the key bits in the example solution described. They must use certified non-deterministic random number generators.

5.7.9 Standardization.

Because the available portable storage media have a USB or SATA interface and the data can be read directly by any operating system, no further standardization is necessary. USB adapters are also available for the SATA interface so that it can also be used with laptops, etc. The TCG-OPAL standard exists for functionality (Chap 5.2.2).

The USB interface is used for random number generators, while the PCIe interface is used for very fast generators; both are also standardized interfaces. However, the PCIe interface usually requires desktop PCs.

5.7.10 Certification

The available portable storage media, random number generators, and HSMs are all comprehensive and certified for high-security applications. Depending on the region, this involves Common Criteria (CC), EUCC, FIPS, etc., i.e., suitable certifications are a matter of course at MKD. From a purely security perspective, particular attention

must be paid to the quality of the random number generators, as they determine the quality of the key and represent the central security component of an MKD solution.

5.7.11 Advantages/Disadvantages of the Technology

The main disadvantage of MKD is that physical transport of the storage media with suitable logistics is required. With few partners, this is not an issue, as this transport is only necessary at longer intervals (months, years) and is easy to implement. With devices such as aircraft, etc., the storage medium can be replaced during maintenance, for example. In a network with n partners or n end devices, $(n^2\text{-}n)/2$ storage media and a maximum of $(n^2\text{-}n)/2$ transports are required for a key exchange. When distributing the storage media, e.g., to company locations, all storage media at a location can be transported at the same time, significantly reducing the number of transports required.

Suitable logistics should always be used for this purpose (see Sect.7.3), but it is essential in many cases when there are a large number of end devices.

MKD requires no maintenance—damaged or old storage media are simply replaced with new ones. MKD is therefore a very durable solution that can also be gradually and cost-effectively converted to new storage technologies and standards (e.g., USB and SATA) without any impact on operations.

The sharp increase in the amount of data in telecommunications and data storage in IT over the past decades, which will continue, is not a problem for MKD with One-Time Pad, because portable storage media, such as SSDs, have always kept pace with this growth and will continue to do so in the future. Therefore, the one-time pad capability of MKD will remain intact in the future.

5.7.12 Man-in-the-Middle Attacks

Passive Man-in-the-Middle

A passive man-in-the-middle attack can be ruled out if the attacker is not located directly next to the storage medium.

Active Man-in-the-Middle

An active man-in-the-middle attack requires the attacker to intercept the portable storage medium during transport and crack the access protection. This is impossible if the medium is transported personally or by a trusted third party (partner).

Transportation by a public service provider allows for an active man-in-the-middle attack. In this case, the storage medium must be destroyed in order to gain direct access to the data. Then the AES-256 encryption of the storage medium must be cracked. If this encryption is not trusted because it is a mathematical process, MKD with a one-time pad must be transported personally or by a trusted third party, because this transport also reliably prevents this attack scenario.

A man-in-the-middle attack directly on the end device is effectively shifted to the one-time pad, where the plaintext data must always be located, and is therefore not an MKD-specific problem.

5.7.13 Authentication

Personal transport or transport by a trusted third party and the PIN and smart card required for access provide two-factor or three-factor authentication. However, even with a public service provider, two-factor authentication with a PIN and smart card is used. Another advantage of MKD with a one-time pad is that authentication can be renewed with each transport, i.e., it is long-lasting.

5.7.14 Integrity / Errors

The integrity of the key, which is a major challenge with QKD and RKD, is a matter of course with MKD with a one-time pad due to the nature of the system.

References

[WP-OTP] Wikipedia contributors "One-time pad," Wikipedia, The Free Encyclopedia, https://en.wikipedia.org/wiki/One-time_pad

[WP-Scy] Wikipedia contributors, "Scytale," Wikipedia, The Free Encyclopedia, https://en.wikipedia.org/wiki/Scytale

[WP-Ste] Wikipedia contributors, "Steganography," Wikipedia, The Free Encyclopedia, https://en.wikipedia.org/wiki/steganography

[Rankl10] W. Rankl, W. Effing, Smart Card Handbook, 4th edn. (Wiley 2010), ISBN: 978–0–470-74367-6, https://www.wiley.com/en-us/Smart+Card+Handbook%2C+4th+Edition-p-9780470743676

[WP-Iso] Wikipedia contributors, "ISO/IEC 7816," Wikipedia, The Free Encyclopedia, https://en.wikipedia.org/wiki/ISO/IEC_7816

[WP-3D] Wikipedia contributors, "Triple DES," Wikipedia, The Free Encyclopedia, https://en.wikipedia.org/wiki/Triple_DES

[WP-HSM] Wikipedia contributors, "Hardware security module," Wikipedia, The Free Encyclopedia, https://en.wikipedia.org/wiki/Hardware_security_module

[Rij22] D. Rijmenants, *The Complete Guide to Secure Communications with the One Time Pad Cipher*, 8.1 edn. (Self-published manuscript, 2022). https://ciphermachinesandcryptology.com/papers/one_time_pad.pdf

[Bell11] S. Bellovin, M. Frank Miller, Inventor of the one-time pad. Cryptologia **35**(3), 203–222 (2011). https://doi.org/10.1080/01611194.2011.583711

[Bor12] S. Borowski, M. Lesniewicz, Modern usage of old one-time pad, in *Military Communications and Information System Conference* (IEEE, 2012), pp. 1–5, https://ieeexplore.ieee.org/abstract/document/6387923

[WP-DH] Wikipedia contributors, "Diffie–Hellman key exchange," Wikipedia, The Free Encyclopedia, https://en.wikipedia.org/wiki/Diffie–Hellman_key_exchange

[Diff22] W. Diffie, M.E. Hellman, New directions in cryptography, in *Democratizing Cryptography: The Work of Whitfield Diffie and Martin Hellman*, (2022), pp. 365–390. https://doi.org/10.1145/3549993.3550007

[WP-PIN] Wikipedia contributors, "Personal identification number," Wikipedia, The Free Encyclopedia, https://en.wikipedia.org/wiki/Personal_identification_number

[WP-Zer] Wikipedia contributors, "Zeroisation," Wikipedia, The Free Encyclopedia, https://en.wikipedia.org/wiki/Zeroisation

[WP-COC] Wikipedia contributors, "Chain of custody," Wikipedia, The Free Encyclopedia, https://en.wikipedia.org/wiki/Chain_of_custody

[WP-Opa] Wikipedia contributors, "Opal Storage Specification," Wikipedia, The Free Encyclopedia, https://en.wikipedia.org/wiki/Opal_Storage_Specification

[TCGOpa] Trusted Computing Group (TCG). "Storage Work Group, Storage Security Subsystem Class: Opal" (specification web page). no date; https://trustedcomputinggroup.org/resource/storage-work-group-storage-security-subsystem-class-opal/

[WP-TCG] Wikipedia contributors, "Trusted Computing Group," Wikipedia, The Free Encyclopedia, https://en.wikipedia.org/wiki/Trusted_Computing_Group

[BSI12] BSI, "Protection Profile for Portable Storage Medie (PSMPP)", Common Criteria Protection Profile, BSI-CC-PP-0081-2012; https://www.commoncriteriaportal.org/files/ppfiles/pp0081b_pdf.pdf

[Vai23] V. Mannalath, S. Mishra, A. Pathak, A comprehensive review of quantum random number generators: Concepts, classification and the origin of randomness. Quantum Inf. Process. Springer Science and Business Media LLC. **22**, Nr. 439 (2023) https://doi.org/10.1007/s11128-023-04175-y

[John18] Johnston, David, *Random Number Generators—Principles and Practices: A Guide for Engineers and Programmers* (Walter de Gruyter GmbH & Co KG, 2018). https://doi.org/10.1515/9781501506062

[Meij19] C. Meijer, B. van Gastel, Self-Encrypting Deception: Weaknesses in the Encryption of Solid State Drives, in 2019 *IEEE Symposium on Security and Privacy (SP)* (IEEE, San Francisco, CA, USA, 2019), pp. 72–87. ISBN 978–1–5386-6660-9. ISSN 2375–1207, https://doi.org/10.1109/SP.2019.00088

[WP-RBA] Wikipedia contributors, "Role-based access control," Wikipedia, The Free Encyclopedia, https://en.wikipedia.org/wiki/Role-based_access_control