Chapter 7
Data Storage, Procurement, Distribution Logistics

This chapter deals with three practical aspects:

1. Data encryption for data storage on PCs.
2. Procurement of QKD, RKD, and MKD products with consideration for IT security.
3. Distribution logistics for MKD: Secure logistics for the distribution of storage media for MKD.

7.1 Role-Based Data Encryption

Data is usually stored in databases or files. Role-based or attribute-based access control systems are typically used for access control. These determine rights such as read, write, and delete. In conjunction with cryptography, cryptographic access control systems are required which, in role-based or attribute-based systems, only recognize encryption/decryption rights, from which read rights in particular can then be directly derived (reading is only possible through successful decryption). Only users (subjects) who have read rights for a specific role receive the corresponding key to decrypt the data that the role contains as objects—they cannot therefore decrypt and read any other data. For reasons of speed, only symmetric methods such as AES or the one-time pad with different encryption modes (see Chap. 6.4) are suitable for encryption/decryption and MAC calculation. In contrast to telecommunications, the keys must be retained for as long as the encrypted data is stored and relevant for reading. This can be many years.

The required keys are determined based on roles/attributes. In a role-based system, each role is assigned a key, which usually originates from administrators (role managers) of the role. When authorized users (subjects) leave a role, a new key must be determined by an administrator of the role. Once all data relevant to this role has been re-encrypted, only the new role key is required. In the other case, which is

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_7

common in decentralized systems, all older role keys must also be retained. In this case, the number of required keys increases constantly. Over the years, this can result in a large number of keys, all of which must be stored securely over a long period of time. For details, see also Chap. 5.3.2.

7.1.1 MKD Solution LISA

There is currently only one product available on the market called "LISA".[1] It is the only product that can fully meet the processes described in Chap. 5.3 and the requirements for MKD (see Chap. 5) and the encryption modes (see Chap. 6.4). LISA is available for PC operating systems and was developed, among other things, to enable the full use of MKD for data storage on desktop PCs, laptops, tablets, etc.

In addition to a solution with smart cards, TPM chips, and AES encryption, LISA also offers completely math-free cryptography (except for the XOR function) with a one-time pad for highly sensitive data through the complete implementation of MKD technology. This applies on a role-based basis to all files and individual elements of the rows and columns of a database. LISA is also available as a LISA workstation with the entire LISA software (see above), in which conventional PCs from the market, e.g., laptops, can be operated with several parallel virtual workstations with different security levels at the operating system level, from open (as is usual for PCs) to closed (highly secure).

7.2 Procurement of QKD, RKD, and MKD Products with Consideration for IT Security

Physical methods always require hardware for implementation in practice. This means that hardware and software are always required for QKD, RKD, and MKD in practical use. With regard to the mathematical methods used in physical methods, strict care must be taken to ensure that all methods used are secure against mathematically very strong opponents and mathematical attack methods that are still unknown (unpublished) today. For a purchaser and user of the devices and software, hereinafter referred to as the product, this is only possible if the mathematical methods used in each product are fully disclosed. Security certifications alone are not sufficient to provide an adequate picture.

Security certifications are important in the high-security sector, but they only cover part of the picture, as successful attacks in the past have shown. They show only a snapshot of a specific environment at the time of certification and not in the user's later overall system or at a later point in time. Past experience has shown that not only have attack scenarios expanded and were not included in the original

[1] https://www.insitu.software

certification process, but that vendors also made changes to the product without new certification. In the past, these changes have also included targeted sabotage and espionage functions. These targeted and significant product deteriorations after certification have also been carried out by reputable providers and in the context of high-security products.

For products (hardware and software from QKD, RKD, and MKD), there is also the problem of supply chains. Hardware and software supply chains are becoming increasingly global and complex, posing major challenges and dependencies for manufacturers, suppliers, and end customers. Multiple components designed, developed, and manufactured in different countries are combined to produce a single piece of hardware or software, which is then purchased by a procurer through a single vendor/supplier. Every player in the global product supply chain has a responsibility to ensure the necessary security and resilience of the product against attacks. However, due to the complexity of the product and the supply chain, effective assurance and verification of defined security are often only possible to a limited extent. This creates the risk that procurers are often unaware of the security level and security vulnerabilities of the products and have no or only limited traceability and control over the products. They may purchase products with integrated sabotage or espionage functions, deliberate vulnerabilities, etc.

The simpler a product is, the more manageable the supply chains and the traceability of security assessments usually are. For example, MKD with One-Time Pad consists of only three main components: the storage media, the random number generators, and the smart cards. In addition, all three of these main components are available as mass-produced goods on the global market. (In terms of hardware, RKD also consists only of mass-produced goods from the global market.) This circumstance has a very positive effect on price, availability/deliverability, maintenance/service, manufacturer/supplier change, and, to a limited extent, security assessments. The smart cards pose the lowest risk because they come from global payment transactions, mobile communications, and passports, which have a very high attack potential, and are certified and regularly tested accordingly. The random number generators are the main component at MKD with the greatest risk of attack and are therefore the central security component. Anyone who succeeds in influencing the generation of random numbers does not need to attack the storage media, the third main component. The random number generators contain an internal mechanism with a few suppliers of subcomponents, which in turn have further suppliers. The entropy of the generated bits (randomness) is the essential performance criterion and can be checked externally, at least to a limited extent, without knowing the current inner workings of a product. From a security perspective, it must also be noted that entropy does not only apply for a limited period of time in order to pass tests. Therefore, checks should also be repeated at a later date. Then there is the danger of artificial radiation that has been deliberately integrated into the product. In MKD, multiple different random number generators are always used, and the random numbers (key bits) are XORed so that an attack or a faulty generator does not affect the key quality (see Sect. 5.2.4). The third and most complex main component in MKD is the storage medium. In terms of security, the main concern here is the AES-256 HW encryption unit. The rest are

MKD-enabled memory sticks or SSDs from the global market. If the key for the internal HW encryption unit is not stored in the storage medium, the only question is whether the encryption unit works according to specifications and does not contain any artificial radiation, etc. Because this is a unit built into the product by a supplier, the supplier must be trusted. Regular monitoring of this supplier by the manufacturer of the MKD-compatible storage medium is important, but often cannot be carried out by the purchaser, or only to a limited extent.

This brief description, which is not yet complete for MKD, shows how quickly complexity can increase and limitations can become insurmountable. RKD is already more complex, and QKD in particular contains a significantly larger number of individual components that come from different suppliers, who in turn require further suppliers, and which can open up security gaps for themselves and the entire product. QKD primarily involves highly complex components such as photon sources, photon detectors, etc., the mathematical methods used for key post-processing and protocols, transmission paths, highly complex trusted nodes, satellites, etc. QKD also enables a variety of side-channel attacks that must be taken into account. QKD is far more complex than MKD and RKD and thus involves issues such as supply chains, the security of individual components and suppliers, etc.

In addition, in the high-security sector, the security offered should also be verifiable by the purchaser at any time, which already poses some challenges with MKD, as mentioned above, with few subcomponents, suppliers, and no mathematical procedures whatsoever.

In the field of high-security cryptography, purchasers are often ministries, military, intelligence services, companies with data that is critical to their survival, etc. who also want to carry out security checks relevant to them at any time—i.e., not only upon initial delivery— and want to have an up-to-date overview of the threat situation at all times.

Therefore, the following minimum requirements have been developed for QKD, RKD, and MKD, which every provider/supplier of a product must offer:

- The product requires the necessary security certifications (CC—Common Criteria, EUCC—European Cybersecurity Certification, FIPS, etc.) from independent, recognized certification institutes.
- Availability of current and time-critical information on vulnerabilities and security risks affecting the product, in particular that providers/suppliers inform purchasers as soon as possible if another customer with the same product identifies and reports any, or if the supplier or one of its suppliers or customers has identified any.
- Disclosure of all known side-channel attacks at the time of the procurement process and later if new ones become known.
- Disclosure of all mathematical procedures and protocols in the product.
- Liability on the part of the provider/supplier and its subcontractors for unreported security vulnerabilities and lack of controls in the supply chain.
- Contractual agreements (service level agreements) with the provider/supplier of a product regarding risk management measures, handling of cybersecurity incidents, and patch management.

In addition to the mandatory requirements listed above, the following recommended requirements are helpful:

- The purchaser should be given sufficient opportunity to conduct its own security checks and security evaluations, which cover the suppliers and their subcontractors and are not limited to the beginning of the life cycle, but can also be carried out regularly at a later stage. To this end, the purchaser should be informed of all components of the product that are critical to security during the procurement process and later, if changes occur. This also includes all components where sabotage or espionage functions and deliberate security vulnerabilities can be integrated.
- Notification of the various suppliers of security-critical components and minimum verifiability of these suppliers (also by purchasers and not only by vendors/suppliers).
- A purchaser should not only know their supplier, but also, upon request, receive relevant information about the entire supply chain affected by security-critical components. In Europe, the EU Supply Chain Regulation [EU24[2]], which is currently the subject of heated debate and controversy, deals with similar aspects, even if the reasons behind it are different. There are many known cases where products have been tampered with during the supply chain by integrating espionage or sabotage functions into the devices during transport. The topic is usually addressed under terms such as supply chain attacks, hardware implants, supply chain manipulation, or hardware tampering [Hua17,[3] Huang17,[4], Perl21[5] Snow19,[6] BSINis2,[7] Scheme n23[8]].

In Europe, the NIS 2 Directive [EU22[9]] requires important and particularly important organizations to implement comprehensive risk management measures. This includes "the security of the supply chain, including security-related aspects of the relationships between the individual organizations and their immediate suppliers or service providers" (Article 21(2)(d) and Article 21(3) NIS 2 Directive).

In the case of QKD, RKD, and MKD products, the supplier or manufacturer of the product determines the security requirements of the product. This means that the purchaser can only make specifications to the supplier or manufacturer during the product selection process, where they compare their security requirements with the products on offer and in terms of the measures to be taken. In the case of these

[2] https://data.europa.eu/eli/dir/2024/1760/oj

[3] doi:10.5555/3153234

[4] https://www.kea.nu/files/textbooks/humblesec/thehardwarehacker.pdf

[5] https://thisishowtheytellmetheworldends.com

[6] https://en.wikipedia.org/wiki/Permanent_Record_(autobiography)

[7] https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Infopakete/NIS-2-Lieferkette/NIS-2-Lieferkette_node.html

[8] https://www.theguardian.com/commentisfree/2013/sep/05/government-betrayed-internet-nsa-spying

[9] https://data.europa.eu/eli/dir/2022/2555/oj

measures, the purchaser often only has comparison options that influence the procurement decision, and they can regulate some aspects of the purchase, leasing, or rental agreement, insofar as this is possible with the supplier. Trust in the supplier and the origin of the product also play a role. The purchaser must be able to rely on the fact that the products delivered have not been tampered with and do not have any hidden functions or deliberately built-in vulnerabilities. A trustworthy supply chain means: verified origin, tested components, and traceable processes. Incidents not only jeopardize sensitive information, but also a company's trust, ability to act, and reputation. The origin of a product and the suppliers (subcontractors) of security-critical components often have a direct influence on the trust placed in the product. One reason for this is the numerous reports and books. Research into such articles gives the impression that products from certain countries are particularly affected by these cases.

Further details on the consideration of security aspects in procurement are described in [Pill16[10]].

7.3 Distribution Logistics

With MKD, key exchange does not take place via telecommunications, e.g., using asymmetric cryptography (e.g., Diffie-Hellman key exchange), or light quanta (QKD), or radio waves (RKD), but rather by transporting the storage media. The storage media can be high-security smart cards, etc. or MKD-enabled portable storage media for encryption with a one-time pad. Therefore, the major challenges of MKD lie in the scaling, organization, and logistical implementation of physical key distribution. 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 to an area characterized by processes, responsibilities, and control.

Therefore, the logistics of distributing storage media play an important role in MKD. In the following, no distinction is made as to whether the storage medium is a smart card or an MKD-enabled storage medium.

This chapter is devoted to this logistics, taking into account not only the distribution of smart cards as key data carriers for mathematical procedures or MKD-enabled storage media with key bits, but also the separate distribution of smart cards used to distribute the key for the internal encryption unit of MKD-enabled storage media. Because MKD is not of interest to the mass market, but primarily to the high-security sector, the number of end devices will usually not be very high in practice, and the distribution of storage media and smart cards will therefore remain manageable. Nevertheless, it must be noted that in telecommunications, each possible pair of

[10] https://www.springerprofessional.de/beschaffung-unter-beruecksichtigung-der-it-sicherheit/12357132

communication partners requires its own key pair, which means a maximum of $(n^2 - n)/2$ key pairs for n end devices.

With MKD, it must also always be borne in mind that cryptographic keys are generated and distributed here, which are then used later to encrypt potentially secret or strictly confidential data. Improper generation of keys or distribution of storage media and smart cards can therefore have legal consequences and cause significant political or economic damage.

The following aspects are discussed below:

- Documented chain of custody (CoC) for MKD.
- Selection by third parties or communication partners.
- Special case of timely distribution (only required for key renewal in the event of subject deletions).
- IT support.

7.3.1 Documented Chain of Custody (CoC) for the Creation and Distribution of Storage Media and Smart Cards

This chapter is completely independent of MKD and of whether the keys are distributed using high-security smart cards or MKD-compatible storage media.

With a CoC, the generation of keys and distribution of key media and smart cards are seamlessly documented, enabling precise tracking. Today, a CoC is essential in areas such as medical devices, forensics, justice, quality management, and supply chain certification, but it is also important for MKD due to its use in high-security areas.

7.3.2 What Does a Documented CoC Include?

It includes the following:

- **Chronological Trail:** Every handover and check is seamlessly documented with a time stamp, location, and responsible person and/or device (laptop, desktop PC, etc.). These processes must be recorded with IT support (e.g., using a smartphone) so that an up-to-date overview can always be accessed. Electronic CoC systems (known as eCOC) are available for this purpose. These processes must be documented flawlessly and in full at all times. Otherwise, tracking is impossible.
- **Identification of the Storage Medium and Transfer Location:** Unique identification, e.g., by means of a QR code (ISO/IEC 18004) or matrix code (ISO/IEC 16022 and 24,720), on all storage media and smart cards, to avoid confusion. In addition, the transfer location must be entered. This can be a terminal

device (laptop, desktop PC, etc., with a QR or matrix code), but also just a location where the storage medium or smart card was handed over. There must be no confusion, because highly secure cryptographic keys are being handed over here. Even though in practice, with MKD-enabled storage media, the actual handover of the keys only takes place via the smart card, the handover of the storage media must also be carried out correctly, or at least be precisely traceable.

- **Responsibilities:** All roles in key generation, distribution and handover of storage media and smart cards, IT processing, etc. must be defined in advance, e.g., via the policy, and it must be possible to determine who did what with which storage media and smart cards and when. All resulting documentation must be traceable and verifiable. This also enables complete auditability of the CoC and, subsequently, the entire generation and distribution of keys at any time.
- **Security Measures:** Access restrictions to the storage media must be defined in advance (e.g., as part of the policy) and, above all, they are technically controlled in a highly secure manner in the real environment via the smart cards that contain the keys for the integrated AES encryption. In addition, the entire IT-controlled input and processing of the CoC must be sufficiently secured so that it cannot be manipulated. Therefore, the most important step when using MKD-enabled storage media is the correct distribution of smart cards, which must be done only once and, if possible, in person by the communication partners in telecommunications and role administrators in data storage. Trusted third parties are also possible here, but should only be the second choice, except for longer distances, and public service providers should absolutely not be allowed.
- **Training of all Parties Involved:** All parties involved, including users of storage media and smart cards, must be adequately trained to ensure that the policy is fully implemented and the CoC is implemented professionally and securely. Training must also be updated.

There are eCoC tools on the market that can detect certain errors in a real eCoC and automatically send out warnings.

7.3.3 Selection by Third Parties or Communication Partners

When storing data with a role-based access control system, the keys are generated by role administrators.

In telecommunications, keys can be generated by the communication partners themselves, but also by selected third parties.

A policy and the exact CoC procedure must be established for the generation and distribution of storage media and smart cards. It must also be specified whether and when public service providers may be used for distribution.

7.3.4 Timely Distribution

This is necessary when a subject leaves a role in a role-based system. In this case, the role key must be replaced with a new one in a solution variant—when using a one-time pad, a larger number of key bits (e.g., 1 TB) must be replaced. This key change must be carried out for all subjects (authorized persons) of the role within a general synchronization pause of a few seconds at a precisely defined point in time. Therefore, when determining this point in time, MKD must take into account the maximum time required for physical key distribution to all active subjects. Currently, passive subjects, e.g., those who are on vacation, can be excluded from this.

7.3.5 IT Support

These processes must be recorded with IT support so that an up-to-date overview can always be accessed. Electronic CoC systems (known as eCoC) are available for this purpose.

For MKD with one-time pads, such an eCoC has just been developed that takes into account all the special features of MKD and supports distribution for storage media and smart cards (see https://cryptography.study/phys/eCoC). Smartphones are used as end devices for the eCoC, and any PC can serve as a server. This solution is to be used in conjunction with the solution described in the chapter "Practical implementation in telecommunications and data storage."

References

[EU24] European Parliament; Council of the European Union. "Directive (EU) 2024/1760 of 13 June 2024 on corporate sustainability due diligence and amending Directive (EU) 2019/1937 and Regulation (EU) 2023/2859." Off. J. Eur. Union, L 2024/1760, (2024). https://data.europa.eu/eli/dir/2024/1760/oj

[Hua17] A. Huang, *The Hardware Hacker: Adventures in Making and Breaking Hardware* (No Starch Press, San Francisco, CA, 2017). https://doi.org/10.5555/3153234

[Huang17] Huang, Andrew, *The Hardware Hacker: Adventures in Making and Breaking Hardware*. (No Starch Press, 2017), ISBN 978–1–59327-758-1. https://www.kea.nu/files/textbooks/humblesec/thehardwarehacker.pdf

[Perl21] N. Perlroth, This Is How They Tell Me The World Ends: The Cyberweapons Arms Race. (Bloomsbury Publishing, 2021), ISBN 9781526629852. https://thisishowtheytellmetheworldends.com

[Snow19] E. Snowden, *Permanent Record*," Metropolitan Books / Henry Holt, (2019), ISBN 978–1250237231. https://en.wikipedia.org/wiki/Permanent_Record_(autobiography)

[BSINis2] BSI. "#nis2know Sichere Lieferkette", (web page), no date; https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/NIS-2-regulierte-Unternehmen/NIS-2-Infopakete/

NIS-2-Lieferkette/NIS-2-Lieferkette_node.html[Schn23] S. Bruce, The US government has betrayed the internet. We need to take it back," (2013). https://www.theguardian.com/commentisfree/2013/sep/05/government-betrayed-internet-nsa-spying

[EU22] European Parliament; Council of the European Union. "Directive (EU) 2022/2555 of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)." Off. J. Eur. Union, L 333, (2022). https://data.europa.eu/eli/dir/2022/2555/oj

[Pill16] E. Piller, *Berücksichtigung der IT-Sicherheit bei der Beschaffung*. (Springer-Vieweg, 2016). https://www.springerprofessional.de/beschaffung-unter-beruecksichtigung-der-it-sicherheit/12357132