Federal Office
for Information Security

BSI – Technical Guideline

Designation:	**Cryptographic Mechanisms: Recommendations and Key Lengths**
Abbreviation:	BSI TR-02102-1
Version:	2022-01
As of:	January 28, 2022

Version	Date	Changes
2017-01	03.01.2017	Fundamental revision of the section on random number generation under Windows. Adjustment of the security level of the present Technical Guideline for the prediction period after 2022 to 120 bits. Corresponding adjustment of the recommended key lengths for RSA mechanisms and DL mechanisms in finite fields.
2018-01	15.12.2017	Fundamental revision of the section on prime number generation. Revision of statements on hash function SHA1 in reaction to the publication of a collision for SHA1. Document history will be limited to the last three years due to space constraints.
2019-01	22.02.2019	Addition of CCM mode among the recommended modes of operation. Addition of PKCS1.5 paddings among legacy mechanisms.
2020-01	24.03.2020	Recommendation of FrodoKEM and Classic McEliece with appropriate security parameters for PQC applications in conjunction with a previously recommended asymmetric mechanism. Recommendation of Argon2id for password hashing. Transitional extension of the conformance of RSA keys with a key length of 2000 bits or more to the end of 2023.
2021-01	08.03.2021	Revision of the chapter on random generators, especially with regard to the use of DRG.3 and NTG.1 random generators. PTG.2 random generators are no longer recommended for general use. Addition of standardised versions of hash-based signature procedures.
2022-01	28.01.2022	Fundamental editorial revision of the entire text, minor adjustments to the layout. Updates in the areas of side-channel analysis, QKD and seed generation for random number generators.

Federal Office for Information Security
P.O.B. 20 03 63, 53133 Bonn, Germany
Email: tr02102@bsi.bund.de
Internet: https://www.bsi.bund.de

Contents

List of Tables

Notations and Glossary

gcd — The greatest common divisor $\gcd(a, b)$ is that natural number with the property that it divides both a and b and that any other natural number also dividing the numbers a and b is already a divisor of $\gcd(a, b)$.

$\mathbb{F}_n$ — Field with n elements, also called Galois field $\mathrm{GF}(n)$.

$\mathbb{Z}_n$ — Ring of residue classes modulo n in $\mathbb{Z}$, also called $\mathbb{Z}/n\mathbb{Z}$.

lcd — The lowest or least common multiple $\mathrm{lcm}(a, b)$ of two integers $a, b \in \mathbb{Z}$ is the smallest positive integer that is both a multiple of a and a multiple of b.

φ — Euler's phi function $\varphi\colon \mathbb{Z} \to \mathbb{Z}$, also known as Euler's totient function, is defined as $\varphi(n) \coloneqq \mathrm{Card}(\{a \in \mathbb{N}\colon 1 \leq a \leq n,\ \gcd(a, n) = 1\}) = \mathrm{Card}(\mathbb{Z}_n^*)$.

R^* — Unit group of the commutative ring R.

Card — Number of elements $\mathrm{Card}(M)$ of a finite set M.

Ceiling function — Ceiling function $\lceil\cdot\rceil\colon \mathbb{R} \to \mathbb{Z}$, defined as $\lceil x \rceil \coloneqq \min\{z \in \mathbb{Z}\colon z \geq x\}$.

Floor function — Floor function $\lfloor\cdot\rfloor\colon \mathbb{R} \to \mathbb{Z}$, defined as $\lfloor x \rfloor \coloneqq \max\{z \in \mathbb{Z}\colon z \leq x\}$.

A

AES — Advanced encryption standard, block cipher standardised by NIST in FIPS 197 [85] with a block size of 128 bits. According to the length of the keys a distinction is made between AES-128, AES-192 and AES-256. Apart from related-key attacks against AES-192 and AES-256, there are no known attacks against AES that provide a significant advantage over generic attacks on block ciphers.

Asymmetric cryptography — Generic term for cryptographic mechanisms in which the execution of some cryptographic operations (such as the encryption of a message or the verification of a signature) can be performed by parties that do not know the secret data.

Authenticated encryption scheme — Encryption schemes that protect not only the confidentiality but also the integrity of the data being encrypted.

Authentication — Objective of secure identification of a person or information-processing system. In the context of the present Technical Guideline, this involves persons or systems that are the source or destination of a communication connection and authentication is realised by making use of a cryptographic secret.

Authentication tag — Cryptographic checksum on data that is designed to reveal both accidental errors and the intentional modification of the data.

Authenticity — Property of veracity, verifiability and reliability of a person, a system or data.

B

Backward secrecy (of cryptographic protocols) Also known as future secrecy or post-compromise security property of a cryptographic protocol that ensures that encrypted messages remain secret even if a key has been compromised in the past.

Birthday problem The birthday problem (also birthday paradox) is the phenomenon that intuitive estimation of certain probabilities is often incorrect. For example, the probability that among 23 people at least two of them have their birthdays on the same day in the year is over 50%, which most people misjudge by a power of ten. In the context of cryptography, this effect plays a role in cryptographic hash functions, among other things, which are supposed to calculate a unique hash value from an input. It is much easier to find two random inputs that have the same hash value than to find another input that has the same hash value as a given one (see also collision attack).

Block cipher Key-dependent, efficiently computable, invertible mapping that maps plaintexts of a fixed given bit length n to ciphertexts of the same length. Without knowledge of the key, it should be practically infeasible to distinguish the output of the block cipher from the output of a random bijective mapping.

Brute-force attack Also called exhaustion method (exhaustion for short); attack method based on an automated, often systematic trial and error of all possibilities, for example to determine secret keys or passwords. If sufficiently long keys are used, brute-force attacks on modern encryption algorithms are practically impossible, as the required computational effort (and thus the time and/or costs) would be too high. Since the performance of modern hardware is continuously increasing and the time required to try out all keys of a certain length is reduced as a result, the minimum key length must be chosen sufficiently large and increased regularly in order to prevent attacks by exhaustion.

C

Challenge-response-authentication Protocol for authenticating to a counterpart on the basis of knowledge. In this process, a verifier poses a challenge which the proving party must solve (response) in order to prove that he knows a certain piece of information without revealing this information itself.

Chosen-ciphertext attack Cryptographic attack in which the attacker can can gather information by obtaining the plaintexts of chosen ciphertexts. The attacker's aim is usually to decipher a given ciphertext that does not belong to any of these plaintext-ciphertext compromises. Depending on whether the attacker knows this ciphertext before or after the end of the attack, a distinction is made between adaptive and non-adaptive chosen-ciphertext attacks.

Chosen-plaintext attack Cryptographic attack in which the attacker can gather information by obtaining the ciphertexts of chosen plaintexts.

Cipher block chaining mode (CBC-mode) Mode of operation of a block cipher in which a plaintext block is XORed with the ciphertext block generated in the previous step before encryption. For secure use, only unpredictable initialisation vectors such as timestamps or a random number must be used.

Collision attack Attack on a cryptolographic hash function with the aim of finding two different input values mapped to an identical hash value. In contrast to preimage attacks, both input values (and thus also the hash value) can be chosen arbitrarily.

Collision resistance A function $h\colon M \to N$ is called collision resistant if it is practically impossible to find $x, y \in M$, $x \neq y$ with $h(x) = h(y)$.

Confidentiality Objective of binding read access to an information to the right of access. In the cryptographic context, this means that access to the content of a message should only be possible for the holders of a secret cryptographic key.

Counter mode (CTR-mode) Mode of operation in which block ciphers can be operated to generate a stream cipher from them. Here, a nonce is encrypted and XORed with the plaintext. The special feature of the counter mode compared to other modes of operation is the fact that the initialisation vector consists of a random number to be newly chosen for each ciphertext block, combined with a counter that is incremented with each further block. The combination can be made, for example, by concatenation, addition or XOR.

Counter with cipher block chaining mode (counter with CBC-MAC, CCM-mode) Mode of operation of a block cipher that combines the counter mode for encryption with the CBC-MAC mode for integrity, thus turning a block cipher into an authenticated encryption algorithm that is capable of guaranteeing both confidentiality and integrity. With CCM, it must be ensured that an initialisation vector is not used twice with the same key, since CCM is derived from the counter mode and the latter represents a stream cipher.

Cryptographic agility, crypto-agility A cryptosystem is considered crypto-agile if it can be replaced by another cryptosystem, for example in terms of cryptographic algorithms, key lengths, key generation schemes or technical implementation, without having to make significant changes to the rest of the overall system.

D

Data authentication Protection of the integrity of a message by means of cryptographic mechanisms.

Dictionary attack Attack method to determine an unknown password (or user name) by systematically trying out a password list (also called wordlist or dictionary). The success of such attacks is based on the fact that user-chosen passwords are often easy to guess in practice, for example if they consist of regular or only slightly modified dictionary entries or are used in a similar form in various places, so that password lists from previous security incidents lead to a successful attack.

Diffie-Hellman-problem (DH) Problem of calculating g^{ab} given g, g^a, g^b in a cyclic group G generated by $g \in G$. The difficulty of this problem depends on the representation of the group. The DH problem is easily solvable by adversaries who are able to calculate discrete logarithms in G.

Discrete-logarithm-problem (DL) Problem of calculating d given g^d in a cyclic group G generated by $g \in G$. The difficulty of this problem depends on the representation of the group.

Disk encryption Complete encryption of a data carrier with the objective that no confidential information can be read from the encrypted system, at least when it is switched off.

DLIES Discrete logarithm integrated encryption scheme, hybrid authenticated encryption scheme based on DH in $\mathbb{F}_p^*$.

E

ECIES Elliptic curve integrated encryption scheme, hybrid authenticated encryption scheme based on DH in elliptic curves.

EME-OAEP Encoding Method for Encryption-Optimal Asymmetric Encryption Padding, padding scheme for RSA, see also OAEP.

Ephemeral key A cryptographic key is called ephemeral if it is generated for each execution of a cryptographic protocol (for example key agreement, signature generation). Depending on the application, further requirements may be imposed on the respective key type, among them uniqueness per message or session.

F

Factorization problem Number theoretic problem in which a composite number is to be decomposed into the product of its prime factors or, more generally, a non-trivial divisor is to be determined.

Fault attack Attack on a cryptographic system in which the attacker uses or actively causes an incorrect execution of a cryptographic operation.

Forward secrecy (of cryptographic protocols) Security property of a cryptographic protocol that states that the disclosure of long-term cryptographic secrets does not enable an adversary to compromise previous sessions of the protocol [44]. It must be noted that for any protocol, forward secrecy can only be reached if a random number generator that guarantees at least Enhanced Backward Secrecy according to [29] was used within the protocol for the generation of the ephemeral keys. If *future* sessions that have not been manipulated by an adversary are also to remain protected in the case that all long-term secrets are compromised, a random number generator that additionally provides Enhanced Forward Secrecy [29] must be used when generating the ephemeral keys.

Forward secrecy (of deterministic random number generators) Security property of a deterministic random number generator that states that future output values of the random number generator cannot be predicted with more than negligible advantage by adversaries who only know previous output values of the random number generator, but not its internal state, and whose computational power is below a limit given by the security level of the deterministic random number generator [29].

G

GCM Galois counter mode, mode of operation for block ciphers, which constructs an authenticated encryption scheme on the basis of a block cipher and supports authentication of non-encrypted data.

GMAC Message authentication code resulting from a use of GCM without data to be encrypted.

H

Hash function Function $h\colon M \to N$ that is efficiently computable and for which M is significantly larger than N. The output of a hash function is called hash value, message digest or simply hash. If h is both collision resistant and resistant to the calculation of first and second preimages, then h is called a *cryptographic* hash function. In the present Technical Guideline, the term *hash function* refers to a cryptographic hash function.

Hybrid encryption Encryption scheme that uses public key cryptography to transport the key for a symmetric encryption method, which is subsequently used to encrypt the message.

I

Information-theoretic security A cryptographic mechanism is called *information-theoretically secure* if any adversary fails in an attempt to break the mechanism due to *lack of information*. In this case, the security objective confidentiality will be achieved irrespective of the computing power available to the adversary, as long as the assumptions about the system information accessible to the adversary are correct. Information-theoretically secure mechanisms exist in many areas of cryptography, for example for the encryption of data (One Time Pad), for the authentication of data (Wegman-Carter MAC), or in the area of secret sharing (Shamir's secret sharing algorithm, see also Chapter 8). Usually there are no security guarantees in mechanisms of this kind if the prerequisites for the operation of the mechanism are not exactly met.

Initialisation vector (IV) Input to a cryptographic primitive used to establish an initial state. Usually, initialisation vectors must be (pseudo-)random, but in some applications it may be sufficient if they are unpredictable or unique.

Instance authentication Proof of the possession of a secret by a user or an information processing system to another party.

Integrity Objective of binding the write access to an information to the right to modify the information. In the cryptographic context, this means that a message can only be changed unnoticed using a certain secret cryptographic key.

K

Key derivation function Cryptographic function that generates one or more other keys from a secret input value, such as a master key, password or passphrase. Key-dependent cryptographic hash functions are commonly used as key derivation functions.

Key length For symmetric cryptographic mechanisms, the key length, also known as key size, is the bit length of the secret key. For RSA (signature and encryption algorithms), the bit length of the RSA modulus n is referred to as key length. For schemes based on the Diffie-Hellman problem or discrete logarithms in $\mathbb{F}_p^*$ (DLIES, DH key exchange, DSA), the key length is defined as the bit length of p. For schemes based on the Diffie-Hellman problem or discrete logarithms in an elliptic curve C over the finite field $\mathbb{F}_n$ (ECIES, ECDH, ECDSA and variants), the key length is the bit length of n.

Key stretching Cryptographic key derivation technique designed to make a weak key, usually a password, more secure by ensuring that more resources (time, memory) are required for brute-force attacks. It must be impossible to calculate the strengthened key from the initial key with less effort.

M

MAC Message authentication code, a key-dependent cryptographic tag. Without knowledge of the key, it should be practically infeasible for an attacker to distinguish the MACs of non-repeating messages from random data. In this case, no adversary can successfully forge tags with a probability considerably above 2^{-t}, where t denotes the length of the authentication tags. Specifications for the length of t depend highly on the given application.

Man-in-the-middle-attack Type of attack in which an attacker inserts himself unnoticed either physically or – nowadays mostly – logically between two or more communication partners in order to, for example, read or manipulate information. The attacker thus enters „in the middle“ of the communication by pretending to be the receiver to the sender and the sender to the receiver.

Min-entropy The min-entropy of a discrete random variable X is defined as $-\log_2(p)$, where p denotes the probability of the most likely value for X.

Mode of operation of a block cipher A mode of operation is a construction to describe how messages longer than the block size of the block cipher are encrypted by the cipher. Only the combination of block cipher and mode of operation allows messages longer than the block length to be encrypted. Usually, the message is divided into several blocks and brought to a suitable length by so-called padding. An initialisation vector can additionally randomise the scheme of the key.

O

OAEP Optimal Asymmetric Encryption Padding, cryptographic padding scheme often used together with RSA encryption. The OAEP is a special form of a Feistel network with which, in the random oracle model, an encryption method that is semantically secure under chosen plaintext attacks can be constructed from any trapdoor function. If used with RSA as trapdoor function, the resulting method is also proved secure against chosen ciphertext attacks. In general, an OAEP achieves the following two goals: It adds an element of randomness which can be used to convert a deterministic encryption scheme into a probabilistic scheme, and it prevents partial decryption of ciphertexts (or other information leakage) by ensuring that an adversary cannot recover any portion of the plaintext without being able to invert the trapdoor one-way permutation.

One-way function Mathematical function that is easy to calculate but difficult to invert. Here, „easy“ and „hard“ are to be understood in the sense of computational complexity theory, specifically the theory of polynomial time problems. In a broader sense, functions are also referred to in this way for which no inversion is yet known that can be computed practically in a reasonable amount of time. A one-way permutation is a one-way function that is also a permutation, that is, a bijective one-way function. Trapdoor one-way functions, also called trapdoor functions, as well as trapdoor permutations represent a special type of one-way functions. They can only be inverted efficiently if some additional information is known. Trapdoor functions are used in asymmetric encryption methods such as RSA.

P

Padding Term for filling messages with *padding data* before encrypting them. Padding is mainly used to bring given data into the format specified by an algorithm or protocol, to randomise the result (for example, the ciphertext or digital signature) of a cryptographic mechanism, or to hide the beginning and end of the relevant data of a transmitted ciphertext.

Partition encryption Partition encryption refers to the complete encryption of a partition of a data medium. The mechanisms used are similar to those used for hard disk encryption.

Pepper Secret string chosen by a server to be appended to a password before calculating a hash value to further complicate dictionary and brute force attacks, also referred to as *secret salt* by NIST. The pepper is not stored in the same database as the hash value, but is stored in a different and as secure as possible place.

Personal identification number (PIN) In the context of this Technical Guideline, a PIN is understood to be a password consisting only of the digits 0-9.

Preimage attack Attack on a cryptographic hash function with the aim of finding a preimage for a given hash value of an unknown input value (first-preimage attack) or to find another preimage for a given input value that provides the same hash value (second-preimage attack).

Preimage resistance A function $h\colon M \to N$ is called preimage resistant if it is practically impossible to find an $x \in M$ with $h(x) = y$ for a given $y \in N$. It is called resistant to calculation of *second* preimages, if for given x, y with $h(x) = y$ it is practically impossible to compute an $x' \neq x$ with $h(x') = y$.

Public-key cryptography See Asymmetric cryptography.

Public key infrastructure System, that can create, distribute, store, verify and revoke digital certificates and is generally used for the management of public keys in the context of asymmetric cryptographic mechanisms.

R

Rainbow table Data structure that allows a fast, memory-efficient search for the original input (usually a password) of a given hash value. The search via a table is considerably faster than with the brute-force method, but the memory requirement is significantly higher (time-memory tradeoff).

Random oracle Theoretical black box that responds to every unique query with a (truly) random response chosen uniformly from its output domain. If a query is repeated, it responds the same way every time that query is submitted. Random oracles are typically used when cryptgraphic proofs cannot be carried out using weaker assumptions on the cryptographic hash function, as due to their construction they fulfill the classical properties of a cryptographic hash function (strong collision resistance and resistance to the calculation of first and second preimages) in a perfect way. A system that is proven secure when every hash function is replaced by a random oracle or a security security proof that uses a random oracle is said to be secure in the random oracle model, as opposed to secure in the standard model of cryptography (the standard model is the model of computation in which the adversary is only limited by the amount of time and computational power available).

Random oracle model See Random oracle.

Related-key attack Attack on a cryptographic mechanism in which an attacker can query encryptions and possibly decryptions not only under the actually used key K, but also under a number of other keys not known to the attacker, which are related to K in a way known to the attacker. This model is very advantageous for the attacker, yet there are situations in which related-key attacks can be practically relevant, for example in the context of constructing a cryptographic hash function based on a block cipher.

RSA Asymmetric cryptographic algorithm (named after its inventors Ronald Rivest, Adi Shamir and Leonard Adleman) that can be used for encryption and digital signatures and is based on the difficulty of the factorisation problem.

S

Salt Randomly chosen string appended to a given plaintext before it is further processed (for example, before input to a hash function) to increase the entropy of the input. Salts are often used for storing and transmitting passwords to make rainbow tables more difficult to use.

Secret sharing A mechanism for distributing secret data (for example a cryptographic key) to several parties or storage media. The original secret can only be reconstructed by evaluating several shared secrets. For example, a secret-sharing scheme may require that at least k of a total of n shared secrets must be known in order to reconstruct the cryptographic key to be protected.

Security Level (of Cryptographic Mechanisms) A cryptographic mechanism achieves a security level of n bits if there are costs associated with each attack against the mechanism that breaks the mechanism's security objective with a high probability of success, equivalent to 2^n calculations of the encryption function of an efficient block cipher (for example, AES).

Seed Start value with which a random number generator is initialised in order to generate a sequence of random numbers or pseudo-random numbers. If the same seed is used in deterministic random number generators, the same sequence of pseudo-random numbers is output.

Shannon entropy The Shannon entropy of a discrete random variable X is defined as $-\sum_{x \in W} p_x \log_2(p_x)$, where W is the range of values of X and p_x is the probability of X taking the value $x \in W$, that is $p_x = \mathbb{P}(X = x)$.

Side-channel attack Attack on a cryptographic system that exploits the results of physical measurements on the system (for example, energy consumption, electromagnetic emanation, runtime of an operation) to gain insight into sensitive data. Side-channel attacks are of very high relevance for the practical security of information-processing systems.

Symmetric cryptography Generic term for cryptographic mechanisms in which all parties involved must have pre-distributed shared secrets in order to be able to perform the entire mechanism.

T

TDEA Triple DES.

Trapdoor one-way function, Trapdoor function, Trapdoor permutation See One-way function.

U

Uniform distribution In the context of this Technical Guideline, *uniformly distributed* generation of a random number from a base set M means that the generating process is practically indistinguishable from an ideally random (that means, from a truly random, equally distributed, independent) drawing of elements from M.

V

Volume encryption See partition encryption.

1. Introduction

In this technical guideline, the Federal Office for Information Security (BSI) provides an assessment of the security of selected cryptographic mechanisms, combined with a long-term orientation for their use. The recommendations made are reviewed annually and adapted if necessary. However, no claim is made to completeness, that means mechanisms not listed are not necessarily considered to be insecure by the BSI. Conversely, it is also wrong to conclude that cryptographic systems which only use the mechanisms recommended in this Technical Guideline as basic components are automatically secure: The requirements of the concrete application and the linking of different cryptographic and non-cryptographic mechanisms can lead to the fact that the recommendations made here cannot be implemented directly or that vulnerabilities arise. Due to these considerations, it must be emphasised in particular that the recommendations made in this Technical Guideline do not anticipate any decisions, for example as in the course of governmental evaluation and approval processes.

This Technical Guideline addresses primarily, in a recommendatory manner, developers who are planning to introduce new cryptographic systems from 2022 onwards. For this reason, this document deliberately refrains from mentioning cryptographic mechanisms which, although still considered secure at the present time, can no longer be recommended in the medium-term, since they show, if not yet exploitable, at least theoretical weaknesses. In the development of new cryptographic systems, various other documents issued by the BSI may also play a role, including [30, 31, 33, 35, 25, 39, 37]. For certain applications, the specifications contained in these documents – in contrast to the recommendations of this Technical Guideline – are binding. A discussion of the regulations contained can be found in [55]. The following two sections first describe the security objectives as well as the selection criteria of the recommended cryptographic mechanisms. Further, very general information on the practical implementation of the recommended mechanisms is given.

The recommended cryptographic mechanisms for the following applications are listed in Chapters 2 to 9:

2 Symmetric Encryption,

3 Asymmetric Encryption,

4 Cryptographic Hash Functions,

5 Data Authentication,

6 Instance Authentication,

7 Key Agreement,

8 Secret Sharing and

9 Random Number Generators.

In the respective sections, the required (minimum) key lengths and other constraints to be observed are stated as well.

Often, various cryptographic algorithms must be combined with each other in order to ensure that a mechanism meets the security requirements placed on it. For example, it is often necessary

not only to encrypt confidential data, but a recipient must also be sure who sent the data and/or whether it was manipulated during transmission. Therefore, the data to be transmitted must additionally be authenticated by means of an adequate method. Another example for the need of the combination of cryptographic primitives are key agreement procedures. Here, it is important to know with whom the key agreement is carried out in order to be able to eliminate so-called man-in-the-middle attacks and unknown key share attacks [14]. This is achieved by schemes which combine key agreement and instance authentication. For these two application scenarios, Annex A specifies corresponding schemes that are constructed by combining the schemes listed in Chapters 2 to 9 and that meet the security level required in this Technical Guideline. In addition, Annex B recommends frequently used functions and algorithms that are required, for example, for key derivation for symmetric mechanisms or for the generation of prime numbers and other system parameters for asymmetric mechanisms. Finally, in Appendix C, recommendations are made for the use of selected cryptographic protocols. In the current version of this Technical Guideline, this only applies to the SRTP protocol; recommendations for TLS, IPsec and SSH have been transferred to the Technical Guidelines TR-02102-2 [22], TR-02102-3 [23] and TR-02102-4 [24] respectively.

1.1. Security Objectives and Selection Criteria

The security of cryptographic mechanisms essentially depends on the strength of the underlying cryptographic primitives. For this reason, this Technical Guideline only recommends mechanisms that can be assessed and evaluated on the basis of the results of many years of analysis and discussion. Other factors of central importance for security are the concrete implementations of the algorithms and the reliability of background systems, such as the public key infrastructures required for the secure exchange of certificates. The realisation of concrete implementations is not considered here, nor are possible problems related to patent law. Even though care was taken in the selection of the mechanism to ensure that the algorithms are free of patents, this cannot be guaranteed by the BSI. In addition, this Technical Guideline contains individual notes to possible difficulties and problems arising during in the implementation of cryptographic mechanisms, but these remarks are not to be understood as an exhaustive list of such problems.

Overall, all cryptographic mechanisms specified in this Technical Guideline achieve a security level of at least 100 bits when used with the parameters specified in the individual sections. For the prediction period after the end of 2022, the use of mechanisms that achieve a security level of at least 120 bits is recommended. However, as a transitional measure, the use of RSA-based signature and confidentiality mechanisms with a key size of at least 2000 bits is still compliant with this Technical Guideline the entire year 2023.[1] The bit lengths recommended in this Technical Guideline for use in new cryptographic systems are based on this minimum level only to the extent that no recommended mechanism falls below it. The effective strength of the recommended mechanisms is in many cases higher than 100 bits. Thus, a security margin against possible future progress in cryptanalysis is provided. As already mentioned before, the converse is not true: mechanisms not specified in this Technical Guideline can nevertheless achieve the required level of security.

Table 1.1 shows the key lengths of selected algorithms and types of algorithms for which a security level of 100 or 120 bits is just achieved according to current knowledge.

[1] If RSA with a key length of less than 3000 bits is used for key transport, the transmitted keys should not be used beyond 2023 (see also Remark 7.1 in Chapter 7).

Symmetric Schemes		Asymmetric Schemes		
Ideal Block Cipher	Ideal MAC	RSA	DSA/DLIES	ECDSA/ECIES
100	100	1900	1900	200
120	120	2800	2800	240

Table 1.1: Examples of key lengths for a security level of at least 100 respective 120 bits.

Table 1.2 summarises the *recommended* key lengths of different types of cryptographic primitives.

Block Cipher	MAC	RSA	DH $\mathbb{F}_p$	ECDH	ECDSA
128	128	2000[a]	2000[a]	250	250

Table 1.2: Recommended key lengths for various cryptographic mechanisms.

[a] For a period of use beyond 2022, the present Technical Guideline recommends using a key length of 3000 bits in order to achieve a comparable level of security for all asymmetric procedures. A key length of $\geq$ 3000 bits will be mandatory from 2023 for cryptographic DLIES and DSA implementations that are to be compliant with this Technical Guideline; for compliance in 2022, a key length of $\geq$ 2000 bits will be sufficient. Transitionally, also the use of RSA-keys with a length of $\geq$ 2000 bits will remain compliant until the end of 2023; from 2024 onwards, an RSA key length of $\geq$ 3000 bits will be mandatory. More detailed information can be found in Remarks 3.2 and 3.3 in Chapter 3.

Key exchange schemes based on Diffie-Hellman are to be handled in Tables 1.1 and 1.2 in accordance with DSA/ECDSA.

In many applications, other security parameters besides the key length play a role in the overall security of a cryptographic system. In the case of message authentication codes (MACs), for example, the length of the digest output is an important security parameter in addition to the key length. Ideally, a MAC should in practice be indistinguishable for an attacker from a random function with a corresponding digest length. As long as this criterion is met, the attacker is left with the option of generating fake messages by guessing, with a per-attempt probability of success of 2^{-n} when n is the tag length. In many applications, $n = 64$ can be considered acceptable in such a situation, that is a tag length of $n = 64$ bits.

In case of block ciphers, the block width is a security parameter independent of the key length. In the absence of structural attacks on a block cipher, the most significant impact of a small block width is that keys have to be exchanged more frequently. The exact impact depends on the used mode of operation. This Technical Guideline does not recommend block ciphers that have a block width of less than 128 bits. An important type of cryptographic primitives that do not process secret data at all are cryptographic hash functions. Here, the length of the digest value returned is the most important security parameter and should be at least 200 bits for general applications to achieve the minimum level of security required by this Technical Guideline. The hash functions recommended in Chapter 4 have a minimum hash length of 256 bits; deviations from this rule for special applications are discussed at appropriate places in this Technical Guideline.

1.2. General Remarks

Reliability of Predictions on the Security of Cryptographic Mechanisms When determining the size of system parameters (such as key length, size of the image domain for hash functions, etc.) not only the best algorithms known today for breaking the corresponding mechanisms and the performance of today's computers have to be taken into account, but above all a forecast of the future development of both aspects, see in particular also [71, 70, 36].

The development of the performance of classical computers can be estimated relatively well today. Fundamental scientific progress (either in terms of attack algorithms or, for example, the development of a cryptographically relevant quantum computer), on the other hand, cannot be predicted. Therefore, any prediction beyond a period of six to seven years is difficult, especially for asymmetric mechanisms, and even for this period of six to seven years, the predictions can turn out to be wrong due to unforeseen developments. The information provided in this Technical Guideline is therefore only limited to a period until the end of 2028.

General Guidelines for Handling Confidential Data with Long-Term Protection Requirements Since an attacker can store data and decrypt it later, there remains a fundamental risk to the long-term protection of confidentiality. This results in the following direct consequences:

- The transmission and storage of confidential data should be reduced to the necessary extent. This applies not only to plaintexts, but also, for example, in particular to the avoidance of storing session keys on any kind of non-volatile media, as well as their undelayed secure deletion as soon as they are no longer needed.

- The cryptosystem must be designed in such a way that a transition to larger key lengths and stronger cryptographic mechanisms is possible (cryptoagility).

- For data whose confidentiality has to remain secure in the long-term, it is recommended to choose for the encryption of the transmission via generally accessible channels such as the Internet, the strongest possible mechanisms of the recommended ones in this Technical Guideline. In most contexts, for example, AES-256 is considered stronger than AES-128 due to its longer key length. However, since such general assessments are difficult – in the concrete example, for example, in some (constructed) scenarios AES-192 and AES-256 are *weaker* than AES-128 against the best known attacks (see [13]) – the advice of an expert should already be sought at an early stage if possible.

- With regard to the selection of cryptographic components for a new application, it should generally be taken into account that the overall system is in general not stronger than the weakest component. Therefore, if a security level of, for example, 128 bits is aimed at for the overall system, all components must at least meet this security level. Selecting individual components that achieve a higher level of security against the best known attacks than the overall system may still make sense under certain circumstances, because this increases the robustness of the system against advances in cryptanalysis.

- In order to minimise the possibility of side-channel attacks and implementation errors, in the case of software implementations of the cryptographic mechanisms presented here, preference should be given to the use of open-source libraries over proprietary developments if it can be assumed that the functions used in the library have been subjected to broad public analysis. When evaluating a cryptosystem, the trustworthiness of all system functions must be assessed; in particular, this also includes dependencies of the solution on properties of the hardware used.

Focus of this Document The security assessment of the cryptographic mechanisms recommended in this Technical Guideline is carried out without taking the concrete use case into consideration. Other security requirements may arise for specific scenarios which may not be met by the mechanisms recommended in this Technical Guideline. Examples include the encryption of storage devices, the encrypted storage and processing of data on systems operated by external providers („Cloud Computing“ or „Cloud Storage“) or cryptographic applications on devices with extremely low computational resources („Lightweight Cryptography“). References to some of the mentioned application scenarios can be found in Section 1.6. This document can therefore support the development of cryptographic infrastructures, but cannot replace the assessment of the overall system by a cryptologist or anticipate the results of such an evaluation.

General Recommendations for the Development of Cryptographic Systems The following list summarises some principles that are generally recommended to be observed in the development of cryptographic systems:

- When planning systems for which cryptographic components are intended, collaboration with experts in the cryptographic field should be sought at an early stage.
- The cryptographic mechanisms listed in this Technical Guideline must be implemented in trusted technical components in order to achieve the required level of security.
- The implementations of the cryptographic mechanisms and protocols themselves must be included in the security analysis to prevent, for example, side-channel attacks or implementation weaknesses.
- If the conformity of a product with the requirements of this Technical Guideline is to be shown, the security of technical components and implementations has to be demonstrated according to the applicable protection profile provided by Common Criteria certificates or similar mechanisms of the BSI, for example in the course of an approval.
- After development and before productive use of a cryptographic system, an evaluation of the system should be carried out by independent experts who were not involved in the development. An assessment of the procedural security by the developers alone should not be considered reliable, even if the developers of the system have good cryptographic knowledge.
- The consequences of a failure of the security mechanisms used must be thoroughly documented. Wherever possible, the system should be designed in such a way that the failure or manipulation of individual system components is detected immediately and the security objectives are preserved by means of a transition to an adequate secure state.

1.3. Cryptographic Remarks

A cryptographic mechanism can often be used for different applications, for example signature methods can be used for both data authentication as well as for instance authentication. In general, different keys should be used for different applications. Another example is symmetric keys for encryption and symmetric data authentication. In concrete implementations, it must be ensured that different keys are used for each of the two mechanisms, which in particular cannot be derived from each other, see also Section A.1.

In some places, this Technical Guideline only provides an informative description of the cryptographic primitives. However, since cryptographic security can only be assessed within the framework of the exact specification and the protocol used in each case, the corresponding standards referred to here must be observed. Further specific information is given, if necessary, in the corresponding sections.

1.4. Implementation Aspects

Besides the cryptanalytic security of the algorithms, the security of their implementation, for example against side-channel and fault attacks, is crucial for the security of a cryptosystem. This is especially true for symmetric encryption methods. A detailed treatment of this topic is beyond the scope of this Technical Guideline, especially since the countermeasures to be taken in individual cases are also highly dependent on the concrete implementation. At this point, only the following general measures are recommended:

- Whenever it is possible with reasonable effort, cryptographic operations should be carried out in security-certified hardware components (for example, on a suitable smart card) and the keys used should not leave these components.
- Attacks that can be carried out by remote, passive attackers are inherently difficult to detect and can therefore lead to significant unnoticed data leakage over a long period of time. These include, for example, attacks exploiting variable bit rates, file lengths or variable response times of cryptographic systems. It is recommended to thoroughly analyse the effects of such side-channels on system security when developing a new cryptographic system and to take the results of the analysis into account in the development process.
- Both attacks on symmetric and asymmetric mechanisms have recently increasingly used attack methods based on mechanisms from the field of machine learning (ML) or artificial intelligence (AI). Neural networks in particular often achieve state-of-the-art results. It is becoming apparent that AI-based methods could be superior to the classic attack methods that are currently most commonly used (for example based on correlations or templates) in some use cases. Therefore, an AI-side-channel guide containing more detailed recommendations on this topic is in preparation.
- At the protocol level, the occurrence of error oracles should be prevented. This can be done most effectively by protecting all ciphertexts by a MAC. The authenticity of the ciphertext should be checked before any other cryptographic operations are performed and no further processing of non-authentic ciphertexts should take place.

As in other contexts, the general recommendation already mentioned several times applies here in particular to always use, wherever possible, components that have already been subjected to intensive analysis by a broad public and to involve experts in the development of new cryptographic systems from an early stage onwards.

1.5. Dealing with Legacy Algorithms

There are algorithms against which no practical attacks are known so far and which still have a high prevalence and thus a certain importance in some applications, but which are basically considered no longer state-of-the-art for new systems. We briefly discuss the most important examples below.

Triple-DES (TDEA) with three independent keys [95] The main arguments against using 3-Key Triple-DES in new systems are the small block width of only 64 bits, the reduced security against generic attacks on block ciphers compared to AES, and various other undesirable properties from a cryptographic point of view. For example, the existence of related-key attacks against Triple-DES with a computation time of $\approx 2^{56}$ Triple-DES computations [67] should be mentioned. Even without considering related-key attacks, Triple-DES has cryptographic properties that do not indicate practically usable weaknesses according to current knowledge, but which are more negative than one would expect for an ideal block cipher with 112 bits effective

key length [75]. Therefore it is recommended not to use Triple-DES in new systems unless it is absolutely necessary for reasons of backward compatibility with existing infrastructure. In this case, too, a migration to AES should be prepared in the foreseeable future.

Overall, triple-DES [95] with two independent keys shows significantly more serious vulnerabilites against Chosen-Plaintext and Known-Plaintext attacks in the single-key setting than Triple-DES with three keys [82, 109]. Even if ultimately no practical attacks against TDEA with two independent keys are known, it is recommended here not only not to use this cipher in new systems, but also to migrate existing crypto mechanisms that use Triple-DES with two keys to AES (or at least to three independent keys) as soon as possible. As far as Triple-DES is still used, all recommendations for use from [95] must be observed.

HMAC-MD5 The lack of collision resistance of MD5 is not yet an immediate problem in the HMAC construction with MD5 as the hash function [9], since the HMAC construction only requires a very weak form of collision resistance from the hash function. However, it seems fundamentally inadvisable to use primitives in new cryptosystems that have been completely broken in their original function. Systems using MD5 for cryptographic purposes are therefore not compliant with this Technical Guideline.

HMAC-SHA1 SHA1 is not a collision-resistant hash function; the generation of SHA1 collisions, while requiring moderate effort, is practically possible [73, 72, 107], even though, according to current knowledge, there are no known weaknesses when using SHA1 in constructions that do not require collision resistance (for example, as the basis for an HMAC, as part of the mask generation function in RSA-OAEP, or as a component of a pseudorandom number generator). However, as a basic security measure, it is recommended to use a hash function of the SHA2 or SHA3 family in these applications as well.

RSA with PKCS1v1.5 padding In principle, it is not recommended to use this format in new systems, neither for encryption nor for signature generation, since there are padding procedures with RSA-OAEP or RSA-PSS with more solid theoretical security properties. In addition, RSA implementations with PKCS1v1.5 padding have proven to be more vulnerable to attacks that exploit side-channel information or implementation errors.

1.6. Other Relevant Aspects

Finally, we would like to explicitly mention some important topics that are either not covered or not covered in detail in this Technical Guideline. The list explicitly does not claim to be complete.

Lightweight Cryptography In this context, particularly restrictive requirements arise with regard to the computing time and memory requirements of the cryptographic mechanisms used. Depending on the application, the security requirements may also differ from the classical ones.

Response Times of a System When using cryptographic mechanisms in areas where tight specifications on the response times of the system must be adhered to, special situations may occur which are not dealt with in this guideline. The recommendations on the use of SRTP in Appendix C cover parts of this topic.

Hard Disk Encryption In the context of hard disk encryption, the problem arises that in most application scenarios neither encryption with data expansion nor a significant expansion of the amount of data that needs to be read from or written to the storage medium is acceptable.

None of the recommended encryption modes is directly suitable as the basis of a hard disk encryption solution. Provided that an attacker cannot combine images of the state of the hard disk at several different points in time, XTS-AES offers relatively good security properties and good efficiency [91]. However, if the attacker can create copies of the encrypted storage medium at a larger number of different points in time, a certain, not necessarily insignificant, leakage of information must be assumed. For example, by comparing two images of a hard disk encrypted with XTS-AES made at different points in time, the attacker can immediately see which plaintext blocks on the hard disk have been changed within this period and which have not.

Disk Encryption of SSD Disks In connection with the encryption of a solid state drive (SSD), it is important to note that the SSD controller does not implement the overwriting of logical storage addresses physically in-place, but distributes them to different physical storage areas. Thus, the current state of an SSD always contains information about certain previous states of the storage medium. An attacker with good knowledge of how the SSD controller works can potentially exploit this to track successive states of a logical storage address. A single image of the encrypted SSD may thus be more valuable to an attacker than a single image of a classical hard disk.

Cloud Storage Similar problems as with the encryption of data media arise with the encrypted storage of entire logical drives on remote systems that are not under the control of the data owner (so-called cloud storage). If the provider of the remote server or its security measures cannot be trusted to a high degree, it must be assumed that an attacker can create disk images at any time without being noticed. If files with sensitive data are stored on a storage system that is regularly under foreign control, cryptographically strong file encryption should be applied before transmission. This also applies if the data is encrypted using volume encryption before it is transferred to the storage medium. The use of a volume encryption solution alone is only recommended if it includes effective cryptographic protection against manipulation of the data and if the other requirements for the use of the corresponding mechanism in general cryptographic contexts are met (for example, the requirement of unpredictable initialisation vectors). In particular, mechanisms should be selected in such a way that, unlike in XTS mode, no significant leakage of information through frequency analysis of successive states is to be expected when a block of data is written repeatedly.

Physical Aspects The present Technical Guideline essentially only addresses those aspects of the security of cryptographic systems that can be reduced to the underlying primitives. Physical aspects such as the emission security of information-processing systems or cryptographic systems whose security is based on physical effects (for example, quantum cryptographic systems) are not or only marginally covered in this Technical Guideline, nor are side-channel attacks, fault attacks and other physical security issues. Any comments in this regard are to be understood explicitly as exemplary references to potential risks without any claim to completeness.

Traffic Flow Analysis None of the mechanisms and protocols for data encryption described in this Technical Guideline achieve by themselves the objective of security against *traffic flow analysis* (so-called *traffic flow confidentiality*). Traffic flow analysis – that is, an analysis of an encrypted data stream taking into account the source, destination, time of existence of a connection, size of the transmitted data packets, data rate and time of transmission of the data packets – can allow significant conclusions to be drawn about the content of encrypted transmissions, see for example [6, 40, 106]. Traffic flow confidentiality is an objective that can usually only be fully achieved with a great deal of effort and is therefore not feasible in many applications that process sensitive information. However, it should be checked in each

individual case by experts to what extent and what kinf of confidential information information is disclosed in a given cryptosystem through traffic flow analysis (and of course other side-channel attacks). Depending on the particular situation, the outcome of such an evaluation may necessitate significant changes to the overall system. It is therefore recommended that the resistance of a cryptographic system to disclosure of sensitive information through traffic flow analysis be considered as an objective from the outset in the development of new systems.

Endpoint Security The security of the endpoints of a cryptographically secured connection is essentially for the security of the transmitted data. When designing a cryptographic system, it must be clearly documented which system components must be trusted to achieve the intended security objectives, and these components must be hardened against compromise in a manner appropriate to the context of use. Appropriate considerations must encompass the entire life cycle of the data to be protected as well as the entire life cycle of the cryptographic secrets generated by the system. Cryptographic mechanisms can reduce the number of components of an overall system whose trustworthiness must be ensured in order to prevent data leakage, but they cannot solve the basic problem of endpoint security.

Quantum-Safe Cryptography Encryption methods may need to protect data once transmitted for a long time. Attacks by future quantum computers should therefore be considered as part of risk management. On the other hand, the standardisation of quantum computer-resistant cryptographic mechanisms has not yet been completed, and at the present time there is also not as much knowledge about their secure implementation as is the case with classical public-key methods. Section 3.2 provides some preliminary recommendations for dealing with issues in this area. An overview of the current state of development of the technology underlying quantum computing can be found in the study [36], among others.

This Technical Guideline does not provide any recommendations, or at least no comprehensive recommendations, with regard to the implementation of mechanisms in the previously mentioned areas. It is therefore advised that in the development of cryptographic systems as a whole – but especially in these areas – experts from the relevant fields should be involved in the development work from the very beginning.

2. Symmetric Encryption Schemes

This chapter deals with symmetric encryption schemes, that is, schemes in which the encryption and decryption keys are identical – in contrast to asymmetric schemes, where the secret key practically cannot be calculated from the public key without additional information. For asymmetric encryption methods, which are usually only used as key transport schemes in practice, please refer to Chapter 3.

Symmetric encryption schemes are used to guarantee the confidentiality of data that is transmitted, for example, via a public channel such as the telephone or Internet. Authenticity and/or integrity of the data is usually not automatically guaranteed. For integrity protection, see Chapter 5 and Section A.1. Even in cases where at first glance the protection of the confidentiality of transmitted data seems to be the dominant or even the only security objective, neglecting integrity-securing mechanisms can easily lead to weaknesses in the overall cryptographic system, which then also makes the system vulnerable to attacks on confidentiality. In particular, such vulnerabilities can arise from certain types of active side-channel attacks, for an example see for instance [110].

2.1. Block Ciphers

General Recommendations A block cipher is an algorithm that encrypts a plaintext of fixed bit length (for example 128 bits) by means of a key to a ciphertext of the same bit length. This bit length is also called *block size* of the cipher. For the encryption of plaintexts of other lengths, block ciphers are applied in different modes, see Section 2.1.1. For new cryptographic applications, only block ciphers whose block size is at least 128 bits should be used.

The following block ciphers are recommended for use in new cryptographic systems:

AES-128, AES-192, AES-256, see [85].

Table 2.1: Recommended block ciphers.

In Version 1.0 of the present Technical Guideline, the block ciphers Serpent and Twofish were also recommended. So far, there are no negative findings on these block ciphers, however, the security of Serpent and Twofish has been examined much less intensively since the end of the AES competition than that of the Rijndael algorithm, which emerged from the competition as the winner and thus future AES. This applies both to classical cryptanalytic attacks and to other security aspects, for example the side-channel resistance of concrete implementations. For this reason, the present version of this Technical Guideline does not recommend any other block ciphers besides AES.

Related-Key Attacks and AES Related-key attacks assume that the attacker has access to encryptions or decryptions of known or chosen plaintexts or ciphertexts under different keys that have a relationship to each other that is known to the attacker (for example, differ in exactly one bit position of the key). Certain attacks of this kind against round-reduced versions

of AES-256 [12] and against unmodified versions of AES-192 as well as AES-256 [13] represent the only known cryptanalytic techniques so far against which AES shows a significantly worse behaviour than an ideal cipher with corresponding key length and block size.

At this point in time, these findings on the security of AES under specific types of related-key attacks have no impact on the recommendations made in this Technical Guideline. In particular, a related-key boomerang attack on AES-256 from [13] with computation time and data complexity of $2^{99.5}$ is not considered to violate the medium-term security level of 120 bits targeted in this Technical Guideline due to the technical prerequisites of related-key boomerang attacks. The best known attacks against AES that do not require related-keys achieve only a slight advantage over generic attacks [17].

2.1.1. Modes of Operation

As mentioned in Section 2.1, a block cipher only provides a mechanism for encrypting plaintexts of a single fixed length. To encrypt plaintexts of arbitrary length, an encryption scheme for plaintexts of (approximately) arbitrary length must be constructed from the block cipher using an appropriate *mode of operation*. Another effect of a cryptographically strong mode of operation is that the resulting encryption scheme will in some respects be stronger than the underlying block cipher, for example if the mode of operation randomises the encryption process, making it difficult to recognise multiple encryptions of the same plaintexts.

Various modes of operation for block ciphers can initially only handle plaintexts whose length is a multiple of the block size. In this case, the last block of a given plaintext may be too short and must be padded accordingly. Formatting by filling this last block to the required block size is also called *padding*. In Section 2.1.3 suitable padding mechanisms are presented. However, among the recommended modes of operation for block ciphers, only the CBC mode requires a padding step.

The simplest way to encrypt a plaintext whose length is already a multiple of the block size is to encrypt each plaintext block with the same key; this mode of operation is also called the Electronic Code Book (ECB). However, the use of the ECB mode of operation leads to the fact that the same plaintext blocks are encrypted into the same ciphertext blocks. The ciphertext thus at least provides information about the structure of the plaintext and, if the entropy per block of the plaintext is low, it may be possible to reconstruct parts of the plaintext by frequency analysis. For this reason, the n-th cipher block should not only depend on the n-th plaintext block and the key used but also on an additional value, such as the $(n-1)$-th ciphertext block or a counter.

This is the case for the following recommended modes of operation, which are adequate for the block ciphers listed in Table 2.1:

- Counter with Cipher Block Chaining Message Authentication (CCM), see [88],
- Galois/Counter Mode (GCM), see [89],
- Cipher Block Chaining (CBC), see [86], and
- Counter Mode (CTR), see [86].

Table 2.2: Recommended modes of operation for block ciphers.

Remark 2.1 Both GCM mode and CCM mode provide cryptographically secure data authentication in addition to encryption if the tag length is sufficient. For the other two modes of

operation, it is generally recommended to provide separate mechanisms for data authentication in the overall system. Ideally, no decryption or other further processing should take place for unauthenticated encrypted data. If unauthenticated encrypted data is decrypted and further processed, then there are increased residual risks with regard to the exploitation of error oracles, see for example [110].

2.1.2. Conditions of Use

The modes of operation listed in Section 2.1.1 require initialisation vectors and furthermore certain other conditions must be met for secure operation, which are summarised below:

For CCM, GCM and CTR mode:

- Initialisation vectors must not repeat within the lifetime of a key. More precisely, no two AES encryptions (that means applications of the underlying AES block cipher) with the same input values (key, message) must ever be performed. Failure to comply with this condition will result in a potentially complete loss of confidentiality for the affected plaintext blocks.

For CCM:

- The length of the authentication tag must be chosen appropriately. For general cryptographic applications, a tag length of ≥ 64 bits is recommended. In general, attackers can modify cipher rate or authenticated data undetected with a success probability of $\approx 2^{-t}$ per attempt when using tag length t in CCM mode. When using tag lengths lower than those recommended here, the associated residual risks must be carefully examined by an expert.

For GCM:

- For GCM initialisation vectors, a bit length of 96 bits is recommended in [89]. This recommendation is followed by the present Technical Guideline, in particular with reference to the results from [65].[1] In [89], it is required that the probability of repetition of initialisation vectors under a given key should be $\leq 2^{-32}$. This implies a key change after at most 2^{32} calls of the authenticated encryption function. If the initialisation vectors are generated deterministically, it must be demonstrated that a repetition of initialisation vectors over the entire lifetime of a key is not possible.
- For general cryptographic applications, GCM with a length of the GCM tags of at least 96 bits should be used. For special applications, shorter tags can be used after consultation with experts. In this case, the guidelines on the number of allowed calls to the authentication function with a common key from [89] must be strictly adhered to.

For CBC:

- Only unpredictable initialisation vectors are to be used.

To generate unpredictable initialisation vectors, various methods are recommended in Section B.2. For applications where the initialisation vector requirements given here cannot be met, it is strongly advised to consult an expert.

[1] In [65], errors in previously accepted security proofs on Galois/Counter mode are pointed out and a corrected analysis of the security of GCM is presented. In this corrected analysis, an IV length of exactly 96 bits turned out to be advantageous.

2.1.3. Padding Schemes

As already explained in Section 2.1.1, the CBC mode requires an additional padding step: it may happen during the partitioning of a plaintext to be encrypted that the last plaintext block is smaller than the block size of the cipher used.

The following padding schemes are recommended in this Technical Guideline:

- ISO-Padding, see [58], Padding Method 2 and [86], Appendix A,
- Padding according to [53], Section 6.3,
- ESP-Padding, see [68] Section 2.4.

Table 2.3: Recommended padding schemes for block ciphers.

Remark 2.2 In CBC mode of operation, care must be taken to ensure that an attacker cannot learn from error messages or other side-channels whether the padding of an introduced data packet was correct [110]. More generally, in encryption schemes where an attacker can make changes to the ciphertext in such a way as to result in controlled changes to the plaintext, no side-channel information must be available to tell whether a given ciphertext corresponds to a valid plaintext or whether it is of invalid format.

2.2. Stream Ciphers

In case of stream ciphers, a key stream is first generated from a key and an initialisation vector, that is, a pseudo-random sequence of bits that is then XOR-added bitwise to the message to be encrypted. At the moment, no dedicated stream ciphers are recommended, but AES in counter mode can be considered a stream cipher. If a stream cipher is used, it is strongly recommended to protect the integrity of the transmitted information by separate cryptographic mechanisms. An attacker can make bit-precise changes to the plaintext in the absence of such mechanisms.

3. Asymmetric Encryption Schemes

Asymmetric encryption methods are usually only used for the transmission of symmetric keys, due to their low efficiency compared to standard symmetric methods, see also Chapter 7. The message to be encrypted (that means, the symmetric key) is encrypted with the public key of the recipient. The recipient can then reverse the encryption with the secret key belonging to the public key. In practice, it must not be possible to reconstruct the plaintext from the ciphertext without knowing the secret key. This implies in particular that the secret key cannot practically be derived from the public key. In order to safeguard the attribution of the public public key to the owner of the corresponding secret key, a public key infrastructure is usually required.

For the specification of asymmetric encryption schemes, the following algorithms need to be specified:

- An algorithm for the generation of key pairs (including system parameters).
- An algorithm for encrypting and an algorithm for decrypting the data.

In addition to recommendations of such algorithms, we also give recommendations on minimum key lengths in this Technical Guideline, see Table 3.1.

In simplified terms, the most practically relevant asymmetric encryption and signature methods are based either on the difficulty of the problem of calculating discrete logarithms in suitable representations of finite cyclic groups (Discrete-logarithm-problem (DL) or on the difficulty of decomposing large integers into their prime factors (Factorization problem). Occasionally, the question arises which of these two approaches is to be considered cryptographically more secure. The present Technical Guideline regards the factorisation of large numbers, the RSA problem, the problem of computing discrete logarithms in suitable fields $\mathbb{F}_p$ (p prime), the problem of computing discrete logarithms in suitable elliptic curves, and the corresponding Diffie-Hellman problems as well-studied hard problems, and there is no reason in this respect to prefer mechanisms based on factorisation to mechanisms based on discrete logarithms, or vice versa. For particularly high security levels, the use of EC mechanisms is advantageous for efficiency reasons, see also Table 3.2.

Remark 3.1 For asymmetric mechanisms, there are usually different equivalent, practically relevant representations of the private and public keys. The bit length of the keys on a storage medium can vary depending on the chosen representation of the keys. For the exact definition of the key length for the recommended asymmetric cryptographic mechanisms, we therefore refer to the entry Key length in the glossary.

The following Table 3.1 provides an overview of the recommended asymmetric encryption schemes and key lengths l in bits.

Scheme	ECIES	DLIES	RSA
Key length l in bits	250	2000[a]	2000[a]
Reference	[1, 56]	[1]	[84]
More detailed information in	Section 3.4	Section 3.5	Section 3.6

Table 3.1: Recommended asymmetric encryption schemes as well as key lengths and normative references.

[a] For a period of use beyond 2022, it is recommended to use RSA/DLIES keys of 3000 bits length to achieve a consistent level of security in all recommended asymmetric encryption schemes. The key length of 2000 bits will remain compliant with this Technical Guideline for DLIES keys until the end of 2022, and also transitionally for RSA keys until the end of 2023. For more details, see the Remarks 3.2 and 3.3.

Remark 3.2 For mechanisms based on the Diffie-Hellman problem/computation of discrete logarithms in elliptic curves, the present conforming key lengths for the period up to 2023 contain a slightly larger security margin compared to the minimum security objectives of this Technical Guideline than is the case for RSA mechanisms. Briefly summarised, this is due to the following reasons:

- The parameter sets for EC mechanisms are standardised, it can therefore be assumed that a given set of security parameters is used for many different applications by a large number of users and thus represents a particularly worthwhile target for attack.
- For *generic* elliptic curves, variants of the Pollard-Rho discrete logarithm computation algorithm are the most efficient known way to solve random instances of the Diffie-Hellman problem. Frequently, however, curve parameters are used in EC mechanisms (for example, for reasons of efficiency) that have obvious non-generic properties or whose generation has only been incompletely documented. It cannot be ruled out that special properties are found for such curves in particular, which make the calculation of discrete logarithms easier than in the generic case.
- The calculation of discrete logarithms in elliptic curves can be parallelised in practice. The parallelisation of the number field sieve (factorisation of large numbers/calculation of discrete logarithms in finite fields) is at least more difficult, especially with regard to the matrix step.

The current recommendations result in only a small buffer between the minimum security level of about 125 bits achieved by the recommended ECC bit lengths and the security level of 120 bits targeted in this Technical Guideline for the period of use from 2023 onwards. In certain applications that have particularly high demands on security or whose security must be guaranteed substantially exceeding the prediction period of this Technical Guideline, it may therefore make sense to provide significantly longer key lengths for EC mechanisms in order to increase the security buffer. The key length requirements of the Country Signer CA from [39], for example, can be explained in this way. Since the security of EC mechanisms depends on the assumption that an attacker cannot use any of the mathematical structure of a given elliptic curve to calculate discrete logarithms faster than the Pollard-Rho algorithm allows, it is conceivable that in the coming years the requirements of the present Technical Guideline will be increased in this area as a basic precaution. It is also recommended as a basic security measure to use curve parameters in EC algorithms that have been generated verifiably at random, whose construction has been comprehensibly documented and whose security has been subjected to a thorough analysis. An example of such curve parameters are the Brainpool curves [74].

Remark 3.3 Based on the factorisation techniques known today, and assuming no use of quantum computers for such attacks, RSA modules of a length of 2000 bits are not expected to be factorised in the near future. However, the security margin of cryptographic mechanisms with an assumed security level of about 100 bits is no longer large once progress of any kind in the field of cryptanalysis is assumed in addition to the development of computational possibilities. In recent years, the use of RSA keys with a higher security level has become technically more feasible. In addition, raising the security level aimed at in this Technical Guideline to 120 bits makes it possible, on the one hand, to harmonise the security margins of the recommended asymmetric mechanisms and, on the other hand, to bring the security objectives of this Technical Guideline closer to corresponding current international regulations, such as the SOGIS crypto catalogue [105]. From the beginning of 2023, the use of 3000 bit keys is therefore recommended as a basic security measure for RSA as well as for cryptographic mechanisms based on the Diffie-Hellman problem in finite fields (DSA, DH key exchange). It is mandatory for systems with a corresponding intended lifetime as a prerequisite for conformity to the present Technical Guideline for DH-based mechanisms from 2023 and for RSA-based mechanisms from 2024 onwards.

Remark 3.4 The asymmetric cryptographic functions recommended in this document require as components further subcomponents, such as hash functions, message authentication codes, random number generators, key derivation functions and/or block ciphers, which in turn must also meet the requirements of the present Technical Guideline in order to achieve the desired level of security. Relevant standards [56] sometimes recommend the use of mechanisms that are not recommended in the present Technical Guideline. In principle, it is recommended to follow two principles when implementing a standard:

- For cryptographic subcomponents, only the respective mechanisms recommended in this Technical Guideline should be used.
- If this is not compatible with standards compliance, an expert must be involved and the final decisions made regarding the chosen cryptographic subcomponents have to be documented in detail and justified from a security point of view.

In the selection of the recommended asymmetric encryption schemes, care has been taken to ensure that only probabilistic algorithms[1] are recommended here. In particular each time a ciphertext is computed, a new random value is needed. Some of the requirements for these random values cannot be met directly by generating equally distributed values of fixed bit length. More details on these random values are given in the sections on the corresponding schemes.

3.1. Asymmetric Key Lengths

3.1.1. General Preliminary Remarks

The assessments of the security of cryptographic mechanisms and key lengths contained in this Technical Guideline are, as already mentioned in the introduction, only valid until 2028. The restriction of the validity of this guideline is of particular importance for asymmetric encryption methods, which is briefly explained below. Furthermore, the question of how the specified key lengths can be derived is briefly addressed.

3.1.2. Security of Asymmetric Mechanisms

The security of asymmetric cryptographic mechanisms is based on the assumed difficulty of problems from algorithmic number theory. In the case of RSA, this is the problem of computing

[1] The RSA algorithm itself is not probabilistic, but the padding method for RSA recommended here is.

e-th roots in $\mathbb{Z}_n$, where $n = p \cdot q$ is a sufficiently large number of unknown factorisation into two prime factors p, q and e is coprime to $\varphi(n) = (p-1)(q-1)$. The security of DLIES and ECIES can be attributed (as far as the asymmetric component is concerned) to the Diffie-Hellman problem in the respective groups used. There are thus reductions to mathematical problems for all recommended mechanisms, which are generally considered as difficult.

However, compared to the situation with symmetric encryption methods, which are in principle also threatened in their long-term security by unforeseen scientific progress, the following aspects should be emphasised:

- With respect to the factorisation problem for general composite numbers and the problem of computing discrete logarithms in $\mathbb{F}_p^*$, there has been greater practically relevant progress since the introduction of asymmetric cryptographic mechanisms than in the cryptanalysis of the most thoroughly studied block ciphers.
- In the case of symmetric algorithms, the threat of active attacks (especially chosen-plaintext and chosen-ciphertext attacks) can be partially offended by appropriate key management, in particular by secure deletion of symmetric keys after their intended lifetime has expired. In addition, if a symmetric cryptographic mechanism shows first signs of vulnerability against plaintext or ciphertext attacks, migration to another mechanism can take place. With asymmetric cryptosystems, on the other hand, at least the public keys associated to the ciphertexts of interest will always be available to an adversary. With the help of this public key, possibly conclusions about the corresponding private key and therewith also on the plaintext can be drawn once a mechanism is broken.
- The asymmetric mechanisms recommended in this Technical Guideline will become insecure in case of significant progress in the development of quantum computers.

Compared to the situation with digital signature algorithms, there is the additional aspect that an attacker can store any ciphertext to which he has access and decrypt it at a later point in time („store-now-decrypt-later“). The objective of ensuring the authenticity of a signed document, on the other hand, can also be ensured retroactively by generating a new signature in a timely manner as long as the evidential value of the old signature algorithm can be considered to be given at the time the new signature is generated. Furthermore, on the legal side, it is possible to no longer accept signatures with cryptographically broken mechanisms at the time of signature verification if no oversignature has been made with a valid mechanism. In contrast, with asymmetric encryption schemes there are usually no subsequent measures to protect the confidentiality of a plaintext to a given ciphertext.

3.1.2.1. Equivalent Key Lengths for Symmetric and Asymmetric Cryptographic Mechanisms

The recommendations of this Technical Guideline on the key lengths of asymmetric cryptographic mechanisms are based on calculations of equivalences of symmetric and asymmetric key lengths, which are based on the following basic assumptions:

- For mechanisms based on elliptic curves: It is assumed that no method exists to solve the Diffie-Hellman problem on the used curve significantly faster than the calculation of discrete logarithms on the same curve. It is further assumed that the computation of discrete logarithms on the elliptic curve used is not possible with significantly less complexity (measured by the number of group operations performed) than for generic representations of the same cyclic group.[2] For a generic group G, a complexity of computing discrete

[2] Algorithms operating on a generic representation of a group have only black-box access to elements and group operations. Intuitively, one can think of something like an oracle that accepts encrypted group elements and outputs the result of group operations in encrypted form.

$\log_2(R)$	ECDLP	Factorisation/DLP in $\mathbb{F}_p^*$
60	120	700
70	140	1000
100	200	1900
128	256	3200
192	384	7900
256	512	15500

Table 3.2: Approximate computational effort R (in multiples of the computational effort for a simple cryptographic operation, for example the one-time evaluation of a block cipher on a block) for the computation of discrete logarithms in elliptic curves (ECDLP) or the factorisation of general composite numbers with the specified bit lengths.

logarithms of $\approx \sqrt{|G|}$ group operations is assumed.

- For RSA and mechanisms based on discrete logarithms in $\mathbb{F}_p^*$: It is assumed that over the prediction period of this Technical Guideline, no attacks become known that are more efficient than the general number field sieve when the parameters are chosen as recommended in this Technical Guideline. For RSA and mechanisms based on discrete logarithms in $\mathbb{F}_p^*$, the same key lengths are recommended. In the case of mechanisms based on discrete logarithms, it is assumed that no mechanism exists to solve the Diffie-Hellman problem in a subgroup $U \subset \mathbb{F}_p^*$ with $\mathrm{ord}(U)$ prime more efficiently than by computing discrete logarithms in U.

- It is assumed that there is no application of attacks using quantum computers.

These assumptions are pessimistic from an attacker's point of view in that they contain no scope for structural progress in cryptanalysis of asymmetric mechanisms. Progress incompatible with the above assumptions may be of a very specific nature and relate, for example, to new insights into *a single* elliptic curve. Although in principle a calculation with 2^{100} elementary operations is not considered practical for the period of time relevant to this Technical Guideline, all recommended key lengths are above the minimum 100-bit security level targeted in this document. For the period from 2023 onwards, a security level of at least 120 bits is consistently being aimed for, although a certain security margin for mechanisms based on elliptic curves remains here as well. For RSA-based mechanisms, the old security level will still be accepted for 2023 as a transitional measure.

With regard to mechanisms whose security is based on the difficulty of calculating discrete logarithms, especially discrete logarithms in elliptic curves, attacks that require oracle access to operations with a user's private key may also be relevant. Such attacks can significantly speed up the calculation of discrete logarithms in a group, see for instance attacks using a static-Diffie-Hellman oracle [20, 41].

For the assessment of runtimes, we follow [45]. In particular, as in [45], we assume that factorising a 512-bit number of arbitrary form is roughly equivalent to the computational cost of 2^{50} DES operations. Using the methods given there – without any security margins for progress in factorisation techniques or techniques for efficient computation of discrete logarithms in the respective groups, respectively – yields approximately the equivalences reproduced in Table 3.2 (compare [45, Table 7.2] and [46, Table 4.1]).

For recommended key lengths, please refer to Table 3.1.

3.1.3. Key Lengths for Information Requiring Long-Term Protection and in Systems with a Long Intended Period of Use

For the purposes of this section, *information requiring long-term protection* means information whose confidentiality is intended to be maintained significantly longer than the period of time for which this Technical Guideline makes predictions about the suitability of cryptographic mechanisms, that means well beyond 2028. A reliable prognosis about the suitability of cryptographic mechanisms over the entire life cycle of a system is no longer possible in this case. It is recommended to provide protection mechanisms that go significantly beyond the minimum requirements of this Technical Guideline with the help of an expert. The following are examples of different ways to minimise risk:

- When developing new cryptographic systems with a projected long period of use, it is advisable to provide for the possibility of future operation with higher key lengths already during development. A possible future need to change the mechanisms used or the implementation of such mechanism changes should also be taken into account during the development of the original system („cryptoagility“).

- Already when introducing the system, higher asymmetric key lengths than required in this Technical Guideline should be used. An obvious option is to aim for a uniform security level of ≥ 128 bits for all system components. Guidance on the minimum asymmetric key lengths required for different security levels can be found in Table 3.2.

- Overall, the amount of information requiring long-term protection that is transmitted over public networks should be reduced to what is absolutely necessary. This applies in particular to information that is transmitted after encryption with a hybrid or asymmetric cryptographic mechanism.

- In the field of quantum computing, there has been significant experimental and theoretical progress in recent years. For the long-term protection of encrypted information, this has resulted in an increasing need for protection against the risk of attacks with quantum computers, provided that public key mechanisms are used for encryption.

  In principle, there are two ways to address the threat posed by quantum computers: On the one hand, one can strengthen a public key mechanism by using a pre-distributed symmetric secret, for example by allowing such a secret to enter into a key negotiation. On the other hand, one can use asymmetric mechanisms for key exchange or key transport that are not vulnerable to attacks with quantum computers.

  The first option is suitable if the required symmetric key material can be reliably and securely distributed in advance to all participants in a communication circle. In that case, the combination of symmetric and asymmetric methods for key transport ensures that attackers can only break the overall procedure if they can both break the underlying mechanism with public keys and know the symmetric secret used.

  The second option solves the problem more fundamentally by using asymmetric cryptography that cannot be attacked by quantum computers, so-called post-quantum cryptography (PQC). This is dealt with in more detail in the next section.

  Depending on the application, the measures to be taken should be considered at an early stage, continuously and adapted to current developments within the framework of risk management.

For a more detailed discussion regarding long-term secure key lengths for asymmetric cryptographic mechanisms that are currently in wide use, we refer to [46, 70].

3.2. Quantum Safe Cryptography

In the following, we address the problem of securing the confidentiality of transmitted data across an insecure network against attackers who have scalable quantum computers (and lots of classical computing power). Addressing this goal is referred to as *post-quantum cryptography*, PQC for short, and the corresponding mathematical mechanisms are also called *PQC encryption mechanisms*. Strictly speaking, PQC confidentiality mechanisms (like other public key encryption mechanisms) usually realise either a secure key exchange or a key transport.

QKD versus PQC Basically, two approaches are being followed in research to ensure communication that is resistant to attacks with quantum computers. On the one hand, the use of quantum physical effects for secure key distribution (quantum key distribution or QKD for short), on the other hand, the use of mathematical PQC encryption methods that can be executed on classical hardware and are based on mathematical problems that, according to current scientific knowledge, cannot be solved efficiently even by quantum computers.

QKD: Features and Applicability The practical restrictions of QKD, such as limited transmission distances and the need to use specialised hardware, are severely limiting compared to the use of PQC mechanisms. Therefore, QKD is only suitable for specific use cases. Furthermore, since no standardised protocols with associated security proofs are available yet, the BSI is not making any recommendations of suitable protocols at this time. As soon as the necessary preconditions are met, the BSI plans to make recommendations on protocols, authentication and the use of QKD in the medium-term. Irrespective of this, the BSI does not and will not recommend the use of the one-time pad alone with keys obtained via QKD or via other key agreement mechanisms in the future either.

Post-Quantum Cryptography There are significantly fewer technical difficulties in the area of PQC mechanisms: In the meanwhile, there exist a number of methods and associated security parameters that appear cryptographically suitable for enabling secure communication links across an insecure network even if attackers have access to quantum computers. The implementation of these mechanisms is possible on standard hardware and the security properties of the resulting systems are basically identical to those of classical public key methods.

However, current PQC mechanisms still have some practical problems: on the one hand, their standardisation has not been completed yet, which means that there are hardly any research results on possible side-channel attacks or implementation flaws compared to classical mechanisms, and on the other hand, relatively large public keys are required. In addition, existing protocols must be adapted to enable the use of PQC cipher suites.

An international standardisation of PQC mechanisms for key transport and signature is to be expected in the next few years within the framework of a corresponding project of the American National Institute of Standards and Technology (NIST). Introducing current, non-standardised mechanisms in new cryptographic systems is therefore always associated with the risk of creating systems that are incompatible with standards that are foreseeable for the near future. In applications that are intended to guarantee the confidentiality of information with a high value and long-term need for protection, however, these problems weigh less heavily in the BSI's view than the possibility of future attacks. In general, it is recommended to put great stress on cryptoagility in the design of new systems; in the context of post-quantum cryptography see in particular also [37].

Grover Attacks on Symmetric Cryptography and Other Attack Models At the present time, there is no evidence that *symmetric* cryptographic mechanisms are threatened in any significant way by quantum computers.

Generally, an adversary which has k universal quantum computers can perform a key-recovery attack against a block cipher with a key length of n bits while executing the Grover algorithm in parallel on all available quantum computers within $\approx \pi 2^{\frac{n-4}{2}}/\sqrt{k}$ time units [51, 111], where one unit of time corresponds to the time needed to execute the block cipher on a quantum computer.

Under the very optimistic assumption that one *unit of time* in the case of AES-128 in a concrete quantum computer implementation corresponds to one nanosecond and that the adversary has to search a key space of size 2^{120} (due to non-ideal random number generation, for example), then an attack with a single quantum computer takes ≈ 30 years. To shorten this to one year, the attacker would have to have ≈ 900 identical quantum computers computing in parallel. In multi-target attacks, the attacker's advantage over classical computers is smaller.

For the foreseeable future, Grover attacks on symmetric cryptographic primitives with the classical security level aimed at in this Technical Guideline therefore do not seem relevant. Practically, they can nevertheless be defended against with little effort by using a higher classical security level; for example, instead of AES-128, AES-256 can be used as a symmetric block cipher. In this case, the requirements for the random sources used must also be adapted accordingly. The use of mechanisms with a classical security level significantly above 128 bits can also be useful in that, for example, the determination of one of l random AES-128 keys generically has an expected overhead of $\approx 2^{127}/l$.

Parts of the literature discuss attacks in which encryption is performed using classical symmetric primitives on quantum computers and attacked in the process, see for example [66]. This attack model is not considered in the present Technical Guideline.

Recommendations The present Technical Guideline gives the following assessments and recommendations, see also [37]:

Recommended Mechanisms: The mechanisms FrodoKEM-976 ([3, Section 2.5]), FrodoKEM-1344 ([3, Section 2.5]) as well as Classic McEliece with the parameters listed in [2, Section 7] in Categories 3 and 5 are assessed to be cryptographically suitable to protect confidential information on a long-term basis at the security level aimed at in this Technical Guideline. This is a very conservative assessment that includes a significant margin of security with respect to future cryptanalytic advances. It is possible that in future revisions of this guideline, other parameter choices and PQC mechanisms may also be deemed technically suitable.

FrodoKEM has not been included among the finalists for the third round of the NIST PQC project, but is considered an alternative candidate. This is mainly due to considerations of the efficiency of the mechanism; there are currently no doubts about its security. The alternative candidates are traded as candidates of a potential fourth round of the PQC project [83]. The BSI therefore maintains its recommendation of FrodoKEM as a PQC mechanism with a high security margin against future attacks. More details can be found in [37].

Combination of Classical and PQC Security: The secure implementation of PQC procedures, especially with regard to side-channel security, avoidance of implementation errors and secure implementation in hardware, and also their classical cryptanalysis are significantly less well studied than for RSA- and ECC-based cryptographic mechanisms. In addition, there are currently no standardised versions of these mechanisms. Their use in productive systems is currently only recommended together with a classic ECC- or RSA-based key exchange or key transport. In this case, one speaks of a so-called *hybrid* mechanism. Parallel to a PQC key transport, an ECC-based key exchange using Brainpool or NIST curves with at least 256 bits key length should be performed. The two shared secrets generated in this way should be combined with the mechanism given in

Section B.1.1 of this Technical Guideline. Here, the standard [98] in its current version explicitly provides the possibility to combine several partial secrets. A hybrid approach, as proposed here, is further described for example in [3] as the most feasible alternative for a use of PQC mechanisms in the near future.

Perfect Forward Secrecy in the PQC context: In principle, it is recommended to use cryptographic mechanisms with perfect forward secrecy if this is technically feasible. In order to achieve *perfect forward secrecy against quantum attackers* in the mechanisms described, fresh public keys must be generated and distributed in an authenticated manner each time a connection is established. After weighing up the additional effort and residual risks, the combined use of a PQC key transport without perfect forward secrecy against quantum attackers with a classic key exchange procedure with perfect forward secrecy against classic attackers may be suitable here. Such mechanisms achieve perfect forward secrecy against classical attackers and protect the users plaintext against reading by quantum attackers *without* access to the PQC long-term key. Attackers *with* access to the PQC long-term key also need a quantum computer in order to decrypt single key establishment sessions.

3.3. Other Remarks

3.3.1. Side-Channel Attacks and Fault Attacks

Depending on the situation at hand, various types of side-channel attacks and/or fault attacks may be relevant to asymmetric encryption schemes and/or asymmetric digital signature schemes. This topic cannot be dealt with comprehensively in the present Technical Guideline. The security of an implementation against side-channel and fault attacks must therefore always be examined on a case-by-case basis. Detailed recommendations on this topic can be found for cryptographic mechanisms based on elliptic curves in [33] and for RSA, $\mathbb{F}_p$-DH and corresponding signature methods in [32].

3.3.2. Public Key Infrastructures

The asymmetric encryption methods described in this Technical Guideline do not in themselves offer any protection against man-in-the-middle attacks. The security guarantees of the described mechanisms are therefore only valid if man-in-the-middle attacks can be reliably prevented by additional mechanisms. For this, an authentic distribution of the public keys of all participants must be ensured.

This can be done in various ways, usually a public key infrastructure (PKI) is used. In a PKI, the problem of authentic distribution of public keys is reduced to the distribution of the root certificates of the PKI. When planning a PKI for an asymmetric encryption or signature procedure, it is recommended to consider the aspects listed below. This is not an exhaustive list of development requirements for public key infrastructures, but merely a list of comparatively generic aspects that are recommended to be considered when developing a PKI; for more information see also [38]. During the development and evaluation of a concrete system, further requirements usually arise, which are not considered here. The development of a suitable PKI for a new cryptographic application is not a trivial task and should therefore only be dealt with in close consultation with appropriate experts.

- When issuing certificates, the PKI should verify that the applicant is in possession of a private key to his public key. This can be done, for example, by a challenge-response mechanism for instance authentication, which requires knowledge of the private key. It is also conceivable to generate the key pairs in an environment that is secure from the PKI's

point of view, if it is combined with a secure transport of the generated key pairs to the end user.

- There should be possibilities for the deactivation of certificates in a timely manner and it should not be possible for an attacker to prevent a verifying party from having the information about the current status of a certificate available at the time of verification without being noticed.
- Certificates should only be issued with a limited validity period.
- All certificate issuers must be trustworthy.
- A certificate should indicate whether it authorises the signing of further certificates. In general, any system that comes into contact with a certificate should be able to clearly determine what this certificate may be used for.
- The length of certificate chains should be limited upwards (by a value as low as possible).

3.4. ECIES Encryption Scheme

An *Elliptic Curve Integrated Encryption Scheme* (ECIES) is a hybrid encryption scheme in which the security of the asymmetric component is based on the Diffie-Hellman problem in the particular elliptic curve used. In the following, we describe a version of ECIES that is compatible with the other recommendations of the present Technical Guideline, closely following [1] in the description of the scheme.

The description of ECIES reproduced here is almost completely identical to the description of the closely related mechanism DLIES in Section 3.5. The main reason for treating the two schemes separately are potential difficulties that could arise from different notations and the different recommendations regarding secure key lengths for the two mechanisms. ECIES-HC in [56] is recommended as a normative reference. For an overview of the standardisation of ECIES and DLIES, we refer to [77].

An ECIES requires the following components:

- Symmetric encryption scheme E_K: All combinations of block cipher and operating mode recommended in this policy are suitable for this purpose.
- Message Authentication Code MAC_{KM}: The mechanisms recommended in Section 5.2 may be used.
- Key derivation function H: For example, H can be a hash function if its output is at least the length of the entire symmetric key material to be derived. Alternatively, the key derivation function recommended in Section B.1 or one of the key derivation functions proposed in [56] may be used to generate derived key material of the desired length from the given data.

In addition, an ECIES requires key material as described in the following section on key generation.

Key Generation

1.) Generate cryptographically strong EC system parameters (p, a, b, P, q, i), see Section B.3.

2.) Choose d randomly and uniformly distributed in $\{1, \ldots, q-1\}$.

3.) Set $G := d \cdot P$.

The EC system parameters (p, a, b, P, q, i) together with G form the public key and d is the secret key. It is recommended to use the curve parameters given in Table B.3.

Encryption Given are a message $M \in \{0,1\}^*$ and a public key (p, a, b, P, q, i, G) that can be reliably assigned to the authorised recipient E of the message. For encryption, the sender S chooses a random number $k \in \{1, \ldots, q-1\}$ and calculates $B := k \cdot P$, $X := k \cdot G$ and from these $h := H(X)$. Sufficiently many bits are taken from h to form a key K for the symmetric encryption method and a key KM for the MAC. From the message M, S computes the ciphertext $C := E_K(M)$ and a MAC $T := \mathrm{MAC}_{KM}(C)$ and sends the triple (B, C, T) to the receiver E.

Decryption Receiver E receives (B, C, T) and calculates $X := d \cdot B$ and therewith $h := H(X)$, K and KM. He determines $T' := \mathrm{MAC}_{KM}(C)$ and checks whether $T = T'$ holds. If it does not, it aborts the decryption process. If $T = T'$, then E recovers the message by $M = E_K^{-1}(C)$.

Key Length For the order q of the base point P should be at least $q \geq 250$.

A necessary condition for the security of the ECIES mechanism is that it is practically impossible to solve the Diffie-Hellman problem in the subgroup generated by P. This is the case for the curve parameters recommended in Table B.3 according to the current state of knowledge.

Remark 3.5 The presented ECIES mechanism is a probabilistic algorithm, since in the second step of the key generation a random number $k \in \{1, \ldots, q-1\}$ must be chosen randomly with respect to the uniform distribution on $\{1, \ldots, q-1\}$. For recommended algorithms for generating the random number k, please refer to Section B.4.

3.5. DLIES Encryption Scheme

A *Discrete Logarithm Integrated Encryption Scheme* is a hybrid encryption scheme where the security of the asymmetric component is based on the difficulty of the Diffie-Hellman problem in a suitable subset of $\mathbb{F}_p^*$. In the following, we describe a version of DLIES that is compatible with the rest of the recommendations in this Technical Guideline, closely following [1] in the description of the scheme.

A DLIES requires the following components:

- Symmetric encryption scheme E_K: All combinations of block cipher and operating mode recommended in this policy are suitable for this purpose.
- Message Authentication Code MAC_{KM}: The mechanisms recommended in section 5.2 may be used.
- Key derivation function H: For example, H can be a hash function if its output is at least the length of the entire symmetric key material to be derived. Alternatively, the key derivation function recommended in Section B.1 or one of the key derivation functions proposed in [56] may be used to generate derived key material of the desired length from the given data.

In addition, a DLIES requires key material as described in the following section on key generation.

Key Generation

1.) Randomly choose a prime q of appropriate bit length (see subsection on key lengths).

2.) Randomly choose k of a bit length that ensures that kq is of the length of the key to be generated. Repeat this step until $p := kq + 1$ is prime.

3.) Choose an $x \in \mathbb{Z}_p^*$ such that $x^k \neq 1 \bmod p$ and set $g := x^k$. Then g is an element of order q in $\mathbb{Z}_p^*$.

4.) Randomly choose a natural number $a \in \mathbb{N}$ with $2 \leq a < q$ and set $A := g^a$.

Then (p, g, A, q) is the public key and a is the secret key.

Encryption Given are a message $M \in \{0,1\}^*$ and a public key (p, g, A, q) that can be reliably assigned to the authorised recipient E of the message. For encryption, the sender S chooses a random number $b \in \{1, \ldots, q-1\}$ and calculates $B := g^b$, $X := A^b$ and from these $h := H(X)$. Suffiently many bits are taken from h to form a key K for the symmetric encryption method and a key KM for the MAC. From the message M, S computes the ciphertext $C := E_K(M)$ and a MAC $T := \mathrm{MAC}_{KM}(C)$ and sends the triple (B, C, T) to the receiver E.

Decryption Receiver E receives (B, C, T) and computes $X := B^a$ and therewith further $h := H(X)$, K and KM. It calculates $T' := \mathrm{MAC}_{KM}(C)$ and checks whether $T = T'$. If this is not the case, the decryption process stops. If, on the other hand, $T = T'$, then E recovers the message through $M = E_K^{-1}(C)$.

Key Length The length of the prime number p should be at least 2000 bits for a period of use until 2022, thereafter at least 3000 bits. The length of the prime q should be at least 250 bits in both cases. Footnote (a) to Table 3.1 and the Remarks 3.2 and 3.3 from Chapter 3 apply accordingly.

A necessary condition for the security of the DLIES mechanism is that it is practically infeasible to determine the discrete logarithm in the subgroup generated by g. This is the case for the recommended size of p and q according to the current state of knowledge. However, the difficulty of the problem of determining discrete logarithms in $\mathbb{F}_p^*$ can be considerably reduced by precomputations that depend only on p and not on the chosen subgroup or its generator. Therefore, as a basic precautionary measure, it is recommended (but currently not mandatory for conformance to the present Technical Guideline) to use key lengths ≥ 3000 bits already before 2023 instead of the minimum required 2000 bits, especially in cases where a large number of users share a common DH modulus.

Remark 3.6 The DLIES mechanism is a probabilistic algorithm, since several random numbers are required during key generation, including a random number $k \in \{1, \ldots, q-1\}$ that must be chosen randomly with respect to the uniform distribution on $\{1, \ldots, q-1\}$. For recommended algorithms for generating the random number k, please refer to section B.4.

Remark 3.7 The efficiency of the key generation mechanism described at the beginning of the section can be increased by having multiple users use the values (p, q, g) so that they can be precomputed once. Alternatively, it is also possible to use published parameters. In this case, the present Technical Guideline recommends using the MODP groups from [69] or the ffdhe groups from [50], in each case combined with the choice of suitable key lengths (this means that, for instance, MODP-1536 is *not* regarded as suitable, independently of the projected period of use). In each of the previously mentioned groups, $q = (p-1)/2$ and $g = 2$. The use of a common p by multiple users is recommended only when $\log_2(p) \geq 3000$, since the computation of discrete logarithms can be simplified by precomputation attacks that depend only on the parameter p.

3.6. RSA

The RSA algorithm, named after its inventors R. Rivest, A. Shamir and L. Adleman, is an asymmetric cryptographic mechanism that can be used for both encryption and digital signing. It uses a key pair consisting of a private key, which is used to decrypt or sign data, and a public key, which is used to encrypt or verify signatures. The security of the mechanism is based on the assumed difficulty of decomposing integers into the product of their prime factors.

Key Generation

1.) Choose two prime numbers p and q randomly and independently of each other. The numbers p and q should be of comparable bit length and not too close to each other. Otherwise if, for example, p and q are chosen independently from a too narrow interval, attacks based on knowledge of the leading bits of p and q are possible.

   More details on the procedure for prime number generation can be found in Section B.5. If p and q are chosen according to Section B.5, the previously mentioned vulnerability does not occur.

   For more details on the procedure for generating prime numbers, see Section B.5.

2.) When using a key length of only 2000 bits, choose the public exponent $e \in \mathbb{N}$ under the constraints

$$\gcd(e, (p-1)\cdot(q-1)) = 1 \quad \text{and} \quad 2^{16}+1 \leq e \leq 2^{1824}-1.$$

3.) Calculate the secret exponent $d \in \mathbb{N}$ as a function of e under the constraint

$$e \cdot d = 1 \bmod \operatorname{lcm}(p-1, q-1).$$

Then (n, e) represents the public key, where $n = p \cdot q$ is the so-called modulus, and d is the secret key. In addition to the secret key d, the two prime numbers p and q must also be kept secret, otherwise everyone would be able to calculate the secret exponent from the public key (n, e) as described under Item 3. It is recommended not to store any data from the key generation persistently except the generated keys and to overwrite all generated data in the computer memory after the key generation. It is further recommended to store the private key on a protected storage medium and/or encrypted in such a way that only authorised users can perform decryption operations.

Remark 3.8 (i) The order of the choice of exponents during key generation, that means first the choice of e and then that of d, is intended to prevent the random choice of small secret exponents, see [18].

(ii) When using probabilistic prime number tests to generate the two primes p and q, the probability that one of the numbers is composite after all should be at most 2^{-100}, see Section B.5 for suitable methods.

Encryption and Decryption For the encryption and decryption, please refer to the standard [84]. It is to be noted that in addition the message must be formatted to the bit length of the modulus n before the secret key d is applied. The formatting procedure must be chosen carefully, the following procedure is recommended:

EME-OAEP, see [84].

Table 3.3: Recommended formatting method for the RSA encryption algorithm.

Using the older PKCS#1v1.5 paddings is not recommended, as variants of Bleichenbacher's attack [15] have repeatedly turned out to be problematic, see for example [16] for a recent example.

Key Length The length of the modulus n should be at least 2000 bits for an expected period of use until the end of 2023. Thereafter, this Technical Guideline requires a key length of at least 3000 bits. Footnote (a) to Table 3.1 and Remarks 3.2 and 3.3 from Chapter 3 apply accordingly.

A necessary condition for the security of the RSA mechanism is that it is practically impossible to decompose the modulus n into its prime factors without knowledge of p and q. With the recommended minimum bit length of 2000 bits, this is the case according to current knowledge.

4. Hash Functions

Hash functions $H\colon \{0,1\}^* \to \{0,1\}^n$ play an important role in many cryptographic mechanisms, for example when deriving cryptographic keys or authenticating data. They map a bit string $m \in \{0,1\}^*$ of arbitrary length[1] to a bit string $h \in \{0,1\}^n$ of fixed length $n \in \mathbb{N}$.

Hash functions used in cryptographic mechanisms, must – depending on the application – meet the following three conditions:

One-Way Property: For given $h \in \{0,1\}^n$, it is practically impossible to find a value $m \in \{0,1\}^*$ with $H(m) = h$.

2nd-Preimage-Property: For given $m \in \{0,1\}^*$, it is practically impossible to find a value $m' \in \{0,1\}^* \backslash \{m\}$ with $H(m) = H(m')$.

Collision Resistance: It is practically impossible to find two values $m, m' \in \{0,1\}^*$ with $m \neq m'$ and $H(m) = H(m')$.

A hash function H satisfying all of the above conditions is called *cryptographically strong*.

these three terms can each be described mathematically more precisely by comparing the best known attacks against these properties with optimal generic attacks. The length of the hash output is a security parameter of crucial importance, as it determines the effort of generic attacks. For the minimum security level required in this Technical Guideline of 120 bits, at least the requirement $n \geq 240$ must be imposed on hash function $H\colon \{0,1\}^* \to \{0,1\}^n$ because of the birthday problem. At this point, it is not necessary to distinguish different cases depending on the period of use of a system, since the hash mechanisms recommended in this Technical Guideline all already have a digest length of ≥ 256 bits.

Remark 4.1 There are cryptographic applications of hash functions in which not all three specified properties of a cryptographically strong hash function are required. Conversely, there are other relevant cryptographic requirements for hash functions that do not follow from the three stated properties. One example is the property of *Zero Finder Resistance* (resistance to the search for preimages of the hash value zero, [19]), which is relevant in the context of ECDSA signatures. All of the hash functions recommended in this Technical Guideline have no known cryptographic weaknesses that are of relevance to the recommended cryptographic mechanisms in which they are used.

According to current knowledge, the following hash functions are considered to be cryptographically strong and are therefore applicable for all mechanisms mentioned in this Technical Guideline:

- SHA-256, SHA-512/256, SHA-384 and SHA-512; see [93].
- SHA3-256, SHA3-384, SHA3-512; see [94].

Table 4.1: Recommended hash functions.

[1] Specifications of real hash functions usually include a length restriction, but this is so high that it is not exceeded by real input strings.

Remark 4.2 The hash function SHA-224 is no longer included in the list of recommended algorithms; on the other hand, with SHA (= SHA2) and SHA3 two families of hash functions are represented. The following comments apply in this respect:

- SHA-224 is to be regarded as a legacy mechanism in the context of this Technical Guideline, but with a security level of about 112 bits it can still be considered as quite strong. The removal is due to the fact that SHA-224 has no advantages over SHA-256 and does not meet the security level of 120 bits aimed at this Technical Guideline for 2023 and beyond.
- Both the hash functions of the SHA2 family and those of the SHA3 family are considered cryptographically strong. With regard to classical attacks on collision resistance and one-way properties, as far as is currently known, there is no practically relevant difference between the two families of functions. In other application scenarios, however, there are differences; the functions of the SHA3 family, for example, are resistant to length extension attacks, see also [8].

Remark 4.3 (i) For the hash function SHA1, examples of hash collisions were first published in [107]. Owing to significant cryptanalytic progress [72, 73], the cost of computing such a collision has since been reduced to order-of-magnitude 10,000 €, and even chosen-prefix collisions are within the reach of academic adversaries. SHA1 should therefore never be used as a secure cryptographic hash function. This does not rule out its use in other cryptographic applications, for example as part of an HMAC construction, but this should also be avoided.

(ii) Even a single collision of a hash function can lead to insecurity in signature algorithms, see for example [76] and [49].

5. Data Authentication

In the context of this Technical Guideline, data authentication refers to cryptographic mechanisms that ensure that data transmitted or stored have not been modified by unauthorised persons and/or applications. For this purpose a prover (usually the sender of the data) uses a cryptographic key to calculate a tag of the data to be authenticated. A verifier (usually the recipient of the data) of the data) then verifies whether the received tag of the data to be authenticated corresponds to the one he would have expected if the data were authentic and the correct key was used.

A distinction is made between symmetric and asymmetric schemes for data authentication. In symmetric schemes, the prover and the verifier use the same cryptographic key. In this case, a third party cannot check who calculated the tag or whether it was calculated correctly. For asymmetric schemes, the private key is used for the calculation of the tag and verified with the associated public key. This is usually implemented by digital signatures (see Section 5.3).

When symmetric methods for data authentication are used, the verifier of a message can in principle also generate forged messages. Thus, such mechanisms are only suitable if the additional risk of compromise resulting from the distribution of the symmetric key and its availability to (at least) two parties is acceptable. In addition, it must be uncritical if the verifying party forges a message. If one of these conditions is not met, symmetric data authentication methods are unsuitable and digital signatures must be used. In scenarios where these properties are unproblematic, the use of symmetric methods is more efficient. A standard scenario in which the use of symmetric methods for data authentication offers itself is the integrity-secured transport of encrypted data over a network after negotiation of ephemeral keys.

5.1. Security Objectives

When using cryptographic mechanisms for data authentication, a clarification of the security objectives to be achieved in the respective scenario is crucial for the selection of the mechanisms. Roughly speaking, the following scenarios can be distinguished, which are important in many applications:

- Ensuring the integrity of data transmitted over a network on the way from the sender to the receiver: In this use case, the sender and receiver usually have a common secret, and the receiver has no interest in producing forged transmissions. The use of a symmetric methods for data authentication is therefore natural.

- Ensuring the non-repudiation of a message: Here it should be ensured that the owner of a particular key can be reliably identified as the originator of a message and that the author himself cannot create a signed message in such a way that doubts can subsequently arise about the validity of the signature. In such situations, the verifier of a message must not have the corresponding signature key, so in this case only the use of digital signatures is possible. In addition, depending on the specific scenario and the sought level of protection, the private signature key may also have to be protected from inspection by the signature provider himself. This is the case, for example, if there is a risk that the signer might subsequently invalidate past signatures by deliberately distributing his own private key. In addition, it must be ensured that the message is displayed to the recipient in the same way as to the creator, and that any unsigned parts (for example, the unsigned subject line

in the case of a signed e-mail) are unambiguously identifiable as such for the recipient as well as for the creator.

- Protection of an asymmetric key exchange against man-in-the-middle attacks: In this use case, no common secret is available, so that integrity-protected transmission of the key exchange messages must be ensured by means of digital signatures.

Remark 5.1 In some application scenarios, there may be special requirements for the security functions involved. For example, a code signature pursues the security objective of the integrity of the transmitted application as well as the non-repudiation of possibly contained malicious functionality in the delivered software, although the signed data can usually neither be meaningfully displayed to the recipient or to the originator nor can their content be checked with reasonable effort. The security functionality of a secure displaying component on the originator's side thus transfers completely to the originator's quality assurance processes and to the security of the technical components used by him.

Remark 5.2 When processing authenticated data, only those data components that have actually been signed must be considered to have data integrity. Enforcing this principle is not always trivial, partly because cases critical to an application may never appear in legitimately signed data. Especially when using more complex signature formats (for example XML signatures) or in contexts where security objectives are to be enforced by digital signatures that were not foreseen during the development of the components used, it should therefore always be thoroughly checked by an expert whether additional safeguards may be required.

Remark 5.3 The authenticity of signed data may still not be sufficiently confirmed by a signature, for example if replay attacks are possible. Such attacks must be prevented by additional measures. In general, this can be achieved by a suitable combination of data authentication schemes with methods for performing challenge-response-based instance authentication. In some situations (for example, software or key updates), checking version counters or timestamps covered by the signature may also be sufficient.

5.2. Message Authentication Code (MAC)

Message authentication codes are symmetric methods for data authentication, usually based on block ciphers or hash functions. They are used when large amounts of data are to be authenticated or when the verification or creation of tags must be particularly efficient for other reasons. The prerequisite in this case is that the proving and the verifying party have agreed on a common symmetric key in advance. Frequently, both the confidentiality as well as the authenticity of the data have to be ensured. Such mechanisms are discussed in Section A.1. In Chapter 7, methods which allow the exchange of keys over insecure channels are presented.

In principle, the following schemes are considered secure if, for the CMAC and GMAC scheme, one of the block ciphers listed in Table 2.1 is used, and for the HMAC scheme one of the hash functions listed in Table 4.1 is used. Furthermore, the length of the key for all schemes should at least be 16 bytes:

- CMAC, see [87],
- HMAC, see [9],
- GMAC, see [89].

Table 5.1: Recommended MAC schemes.

When using these schemes, the following aspects must be observed:

- A tag length of ≥ 96 bits is recommended for general cryptographic applications in all three schemes, with 64 bits as an absolute minimum for general applications. Shorter tag lengths may only be used after experts have weighed up all the circumstances affecting the application in question. For GMAC tags, there are forgery attacks with a success probability of $2^{-t+\log_2(n)}$ per attempt known, where t denotes the tag length and n is the number of blocks of the message. and This probability increases further upon detection of successful forgeries [47]. This means that GMAC (and thus also the authenticated encryption mode GCM) provides weaker integrity protection for the same tag length than is expected for CMAC or HMAC with the respective block ciphers or hash functions recommended in this Technical Guideline. The practical relevance of these attacks increases considerably when short authentication tags (< 64 bits) are used. The use of short tags with GMAC/GCM is therefore strongly discouraged.
- The authentication keys used must be protected in an equally safe manner as other cryptographic secrets in the same context.
- In general, all requirements from [9, 87, 89] must be met in the respective scheme used and their compliance must be documented.

With regard to the GMAC scheme, the other remarks on the operating conditions for GCM from Section 2.1.2 apply accordingly as far as the authentication function is concerned. The following table summarises the recommendations on key and checksum length when using MAC mechanisms:

Scheme	CMAC	HMAC	GMAC
Key length	≥ 128	≥ 128	≥ 128
Recommended tag length	≥ 96	≥ 96	≥ 96

Table 5.2: Parameters for recommended MAC schemes.

5.3. Signature Algorithms

In signature algorithms, the data to be signed is first hashed before the tag and/or the signature is calculated with the secret key of the proving party from this hash value. The verifier then checks the signature with the corresponding public key. As with asymmetric encryption schemes, it must not be possible to calculate the signature without knowledge of the secret key. This implies in particular that it must not be practically possible to derive the secret key from the public key.

To distribute the public keys to the verifiers, usually a public key infrastructure is used. In any case, a reliable way (protected against manipulation) to distribute the public keys is essential, as with all public key schemes. However, an in-depth discussion of the technical and organisational options for solving this problem exceeds the scope of this Technical Guideline, so the topic is only considered in the margins.

For the specification of signature algorithms, the following algorithms are to be specified:

- An algorithm for the generation of key pairs.
- A hash function that maps the data to be signed to a data block of fixed bit length.
- An algorithm for the signing the hashed data and an algorithm for the verification of the signature.

Basically all of the hash functions listed in Table 4.1 are suitable for the calculation of the hash value, so it remains to specify the algorithms and key lengths listed under the first and third point, respectively. In addition, we give recommendations for minimum key lengths.

Table 5.3 provides an overview of the signature methods recommended in the following. All recommended mechanisms can be used for signing data as well as for issuing certificates.

1.)	RSA, see [57]
2.)	DSA, see [60] and [92],
3.)	DSA variants on elliptic curves:
	(a) ECDSA, see [35],
	(b) ECKDSA, ECGDSA, see [35, 60], and
4.)	Merkle signatures, more precisely XMSS+ or LMS and their multi-tree variants according to [54, 78, 97].[a]

Table 5.3: Recommended signature algorithms.

.

[a] Merkle signatures differ in essential points from the other signature algorithms recommended here. For a more detailed description of the most important aspects, see Section 5.3.4

According to the current state of knowledge, with a suitable choice of security parameters, all signature mechanisms recommended here achieve a comparable level of security if the private keys are reliably kept confidential and, in particular, cannot be determined by exploiting implementation weaknesses, such as for instance side channels, fault attacks or mathematical attacks directed against a specific kind of key generation. For the generation of qualified electronic signatures within the scope of application of the Trust Services Act, formally different regulations may apply despite the fact that from a security technical point of view all recommended mechanisms are suitable. We refer to the SOGIS guidance [105] for further information on the suitability of cryptographic algorithms.

Remark 5.4 With the exception of DS 3 (compare Table 5.4) the recommended asymmetric signature algorithms are probabilistic algorithms.[1] Thus, each time a signature is calculated, a

[1] The RSA algorithm itself is deterministic, but not the here recommended padding procedures to RSA (except DS 3).

new random value is required; further requirements for these random values are specified in the corresponding sections.

Remark 5.5 Merkle signatures, unlike all other signature algorithms listed in this Technical Guideline, are considered secure against attacks using quantum computers [21]. Moreover, they are the only scheme mentioned here that is *forward secure* in the sense of [10], see also [64] for more information on forward security.

5.3.1. RSA

The security of the RSA scheme is based on the assumed difficulty of calculating e-th roots in $\mathbb{Z}_n$, where n is an integer of unknown factorisation into two prime factors p, q and e is an exponent coprime to $\varphi(n) = (p-1)(q-1)$.

Key Generation The key generation is analogous to that of the RSA encryption scheme, for details see Section 3.6. The signature verification key is of the form (n, e), where $n = p \cdot q$ is composite, e is invertible modulo $\varphi(n)$ and $2^{16} < e < 2^{256}$, and the signature key is $d := e^{-1} \bmod \varphi(n)$.

Generation and Verification of Signatures For signature generation and/or verification we refer to [57]. Here, the hash value of the message must be padded to the bit length of the module n before the secret key d is applied. The padding scheme must be chosen carefully (see for example [42]); the following schemes are recommended:

- EMSA-PSS, see [84].
- Digital Signature Scheme (DS) 2 and 3, see [62].

Table 5.4: Recommended padding schemes for the RSA signature algorithm.

Key Length The length of the modulus n should be at least 2000 bits for a period of use until 2023 and at least 3000 bits if used beyond 2023. Footnote (a) to Table 3.1 and the Remarks 3.2 and 3.3 from Chapter 3 apply accordingly.

5.3.2. Digital Signature Algorithm (DSA)

The security of the DSA method is based on the assumed difficulty of calculating discrete logarithms in $\mathbb{F}_p^*$.

Key Generation

1.) Choose two prime numbers p and q such that $q \mid (p-1)$.

2.) Choose $x \in \mathbb{F}_p^*$ and calculate $g := x^{(p-1)/q} \bmod p$.

3.) If $g = 1$, go to 2.).

4.) Choose a number $a \in \{1, \ldots, q-1\}$ and set $A := g^a$.

Then (p, q, g, A) is the public key and a is the secret key.

Generation and Verification of Signatures For the signature generation and verification we refer to [60] and [92]. Both signature generation and signature verification require a cryptographic hash function. One of the hash functions recommended in this guideline should be used and the length of the hash values should correspond to the bit length of q. If none of the hash functions recommended in Table 4.1 has a suitable hash length, the q leading bits of the hash output should be used. If the length L_H of the hash value is *shorter* than the bit length of q, the resulting signature algorithm will have a security level of (at most) $L_H/2$ bits.

Key Length The length of the prime number p should be at least 2000 bits for a period of use up to and including 2022. For signatures that are to remain valid without further measures (for instance signature renewal) beyond the end of 2022, a key length ≥ 3000 bits is recommended.

Remark 5.6 The DSA method is a so-called probabilistic algorithm, since a random number $k \in \{1, \ldots, q-1\}$ is needed to calculate the signature. Here, k should be chosen with respect to the uniform distribution on $\{1, \ldots, q-1\}$, since otherwise attacks exist, compare [101]. Two algorithms for calculating k are presented in Section B.4.

Remark 5.7 Regarding the generation of the system parameters, see Remark 3.7.

5.3.3. DSA Versions based on Elliptic Curves

The security of these mechanisms is based on the assumed difficulty of calculating discrete logarithms in elliptic curves.

Key Generation

1.) Generate cryptographically strong EC system parameters (p, a, b, P, q, i), see Section B.3.

2.) Choose d randomly and uniformly distributed in $\{1, \ldots, q-1\}$.

3.) Set $G := d \cdot P$.

Then the EC system parameters (p, a, b, P, q, i) together with G form the public key and d the secret key.

Generation and Verification of Signatures The following algorithms are recommended in this Technical Guideline:

- ECDSA, see [35].
- ECKDSA, ECGDSA, see [35, 60].

Table 5.5: Recommended signature algorithms based on elliptic curves.

For the generation and verification of signatures, a cryptographic hash function is required. In general, all hash functions recommended in this Technical Guideline are suitable. The length of the hash values should correspond to the bit length of q. The other remarks on the choice of hash function from Section 5.3.2 apply accordingly.

Key Length All signature algorithms listed in Table 5.5 ensure a security level of n bits if $q \geq 2^{2n}$ holds for the order q of the base point P and it is assumed that the calculation of discrete logarithms on the curves used is not possible more efficiently than with generic mechanisms. It is recommended to choose $q \geq 2^{250}$.

Remark 5.8 Like the DSA scheme, all of the signature algorithms recommended in this section are probabilistic algorithms. Here too, a random value $k \in \{1, \ldots, q-1\}$ must be chosen according to the uniform distribution on $\{1, \ldots, q-1\}$, since otherwise attacks exist, compare [101]. Two methods for calculating k are presented in Section B.4.

5.3.4. Merkle Signatures

In contrast to the signature algorithms described so far, the security of the signature methods described in [54, 97, 78] is based only on the cryptographic strength of a hash function and a family of pseudorandom functions, but not on the assumed difficulty of a mathematical problem (like the determination of a prime factorisation or the calculation of discrete logarithms in selected groups). In particular, no assumptions on the absence of efficient algorithms for these problems from algorithmic number theory are required. According to current knowledge it is therefore generally assumed that, unlike the other signature methods recommended in this Technical Guideline, Merkle signatures are also secure against attacks using quantum computers.[2]

The generally low complexity-theoretic assumptions underlying the security of Merkle signatures make Merkle signatures appear to be a good scheme for the generation of long-term secure signatures. This is also true under the assumption that attacks by quantum computers are not used during the period of time in which the signature is to remain valid.

However, when using Merkle signatures – unlike in case of the rest of the signature methods described in this Technical Guideline – only a limited number of messages can be authenticated with a given public key. With the single-tree variants XMSS+ and LMS, the computing time for generating the public key is proportional to this maximum number of messages that can be authenticated with a key pair and is thus comparatively long. If a large number of messages are to be signed without intermediate generation and authenticated distribution of a new public key, the use of the multi-tree variants XMSS^MT and HSS is recommended.

5.3.5. Long-Term Preservation of Evidentiary Value for Digital Signatures

If the intended period of time over which the authenticity and integrity of the data to be protected by means of a data authentication system is to remain secure significantly exceeds the prediction period of this Technical Guideline, it is irrespective of the present recommendations on mechanisms and key lengths for digital signatures recommended to take into account the possibility of a future migration of the system to new signature algorithms or longer signature keys already during the development. This should include mechanisms for the signature renewal of old signed documents using the updated schemes. More information on this topic can be found in Technical Guideline TR-03125 (TR-ESOR) [26].

[2] A discussion of quantum security of the collision resistance of hash functions can be found in [11].

6. Instance Authentication

In this Technical Guideline, instance authentication refers to cryptographic protocols in which a prover confirms to a verifier the possession of a secret. For symmetric mechanisms, this secret is a symmetric key, which has to be exchanged in advance. In case of instance authentication with asymmetric mechanisms, the proving party shows that he is in possession of a secret key. A PKI is usually required for this, so that the verifier can assign the corresponding public key to the proving party. Password-based schemes are primarily used to unlock smart cards or other cryptographic components. Here, the owner of the component proves that he is in possession of a password or PIN.

Authentication should – where reasonable and possible – be mutual and can be accompanied by key agreement to ensure the confidentiality and integrity of any subsequent communication, see Chapter 7 for recommended key exchange and key agreement schemes and Section A.2 for recommended protocols that combine both schemes.

In this chapter, for the first two schemes (Sections 6.1 and 6.2), only general ideas about instance authentication are provided and the corresponding cryptographic primitives are recommended. For the required cryptographic protocols it is referred to Section A.2. In particular, among others recommendations for key lengths can be found there.

6.1. Symmetric Schemes

The possession of the secret key is demonstrated by the prover (P) to the verifier (V) by sending a random value r to V. For the scheme to reach the minimum security level aimed at in this Technical Guideline, r should have at least 100 bits of min-entropy. If a large number of authentications are performed with the same secret key, then the probability of a collision of two of these challenge values should be limited to $\leq 2^{-32}$. P uses the shared key K to calculate an authentication code for the message r and sends it back to V, who verifies it. Such schemes are also called *Challenge-Response Methods*, see Table 6.1 for a schematic representation.

Prover (P)		**Verifier (V)**
		Choose random value r
	$\xleftarrow{r}$ (Challenge)	
Calculate authentication code c		
	$\xrightarrow{c}$ (Response)	
		Verify authentication code

Table 6.1: Schematic representation of a Challenge-Response method for instance authentication.

The calculation and verification of the authentication code depends on the selected scheme. In principle, all encryption schemes recommended in Chapter 2 and all MAC schemes recommended in Section 5.2 can be used. For recommended bit lengths and constraints on the random values used, see Section A.2.

6.2. Asymmetric Schemes

Also for asymmetric mechanisms, challenge-response protocols are used for instance authentication. Here, the prover uses his secret key to calculate a tag for a random value r sent by the verifier. The verifier then verifies the tag with the help of the corresponding public key. In general, all of the schemes recommended in Section 5.3 can be used for this purpose. For recommended bit lengths and constraints on the random values used, see also Section A.2.

Remark 6.1 Even though the signature algorithms recommended in Section 5.3 for data authentication can also be used for instance authentication, it has to be ensured that the used keys are different, meaning that a key used to generate signatures is not used for instance authentication. This must also be indicated in the corresponding certificates for the public keys.

6.3. Password-Based Methods

Passwords for unlocking the cryptographic keys made available on cryptographic components (for example signature cards) are usually short, so that the owner of the component can remember the password. In many situations, the permitted character set is also restricted to the digits 0-9; in this case, one also speaks of PIN instead of password. In order to nevertheless reach an adequate security level, the number of access attempts is usually limited.

6.3.1. Recommended Password Lengths for Access to Cryptographic Hardware Components

The following constraints for password lengths and number of attempts for access to cryptographic hardware components are recommended:

- It is generally recommended to use passwords with an entropy of at least $\log_2(10^6)$ bits. This can be achieved, for example, by assigning ideally random six-digit PINs.
- The number of consecutive unsuccessful access attempts must be tightly limited. With a password entropy of $\log_2(10^6)$ bits, a limit of three attempts is recommended.

Table 6.2: Recommended password lengths and number of access attempts for access protection of cryptographic components.

Remark 6.2 If access passwords for cryptographic components are not (at least approximately) ideally randomly generated by a technical process, but chosen by the user, it is strongly recommended to raise the user's awareness with respect to the choice of secure passwords. Furthermore, it is recommended in this case to refrain from using purely numeric passwords (PINs). For passwords formed over an alphabet containing at least the letters A-Z, a-z, 0-9 and, if applicable, special characters, a length of eight characters is recommended. In addition, it is recommended to take safeguards to exclude passwords that are easy to guess (for example, individual words in the respective national language or an important foreign language and dates in easy guessable formats).

Remark 6.3 In some applications, after consideration of all the circumstances by an expert, the use of passwords with lower entropy than recommended above may also be compliant with this Technical Guideline. However, a single unauthorised access attempt should at least never succeed with a probability of success greater than $\approx 10^{-4}$. The number of consecutive unsuccessful access

attempts must be tightly limited, where the exact limitations depend on the application. The residual risks should be thoroughly documented and it is recommended to inform the authorised user of any unauthorised access attempts, if possible, even if the component was not blocked subsequently.

Remark 6.4 (i) To prevent denial-of-service attacks or accidental blocking of the component, there must be a mechanism to unblock the blocking. The entropy of the *personal unblocking key* (PUK) should be at least 100 bits if offline attacks are possible.

(ii) If no offline attacks on the PUK are possible, it is recommended to use a PUK with a min-entropy of 32 (for example 10 digits) and to irrevocably delete the cryptographic secrets contained in the component after a relatively low number of access attempts (for example 20).

(iii) The general recommendation of at least about 20 bits of entropy for the password used in a password-based authentication scheme applies only to authentication to a security component that does not allow of offline attacks and that can reliably enforce the stated restrictions on the number of access attempts allowed. In other situations where these conditions are not met (for example, when a cryptographic secret is directly derived from the password that provides access to sensitive information), it is recommended to choose passwords via a method that offers at least 100 bits of entropy. For access to data or for authentication of transactions with high protection requirements, single-factor authentication is generally not recommended. Instead, two-factor authentication by means of knowledge (knowing a password) and ownership (of a secure hardware component) is recommended in this situation.

6.3.2. Recommended Method for Password-Based Authentication to Cryptographic Hardware Components

For contact-based chip cards, cryptographic protection of the transmission of the PIN to the chip card can currently be omitted if the card terminal itself can be considered as trustworthy and a physical tapping or manipulation of the information transmitted between reader and card is prevented by suitable measures in the operational environment. However, cryptographic protection (with regard to integrity and confidentiality of the transmitted identification data) is also recommended here. In principle, the same mechanisms as for contactless cards are suitable for contact-based cards as well.

In the case of contactless chip cards, the communication between the card reader and the chip card can be read from a distance. Here, the password for activating the chip cannot simply be sent from the card reader to the chip card.

The following password-based method is recommended for the access protection to contactless chip cards:

PACE: Password Authenticated Connection Establishment, see [34].

Table 6.3: Recommended password-based method for the protection of access to contactless chip cards.

The method recommended in Table 6.3 not only demonstrates to the contactless chip card that the user is in possession of the correct password, but at the same time performs a key agreement method, so that subsequently a confidential and authenticated communication can take place.

Remark 6.5 Also with the method recommended in Table 6.3, the number of attempts must be limited. It is recommended to block the chip card after three unsuccessful attempts. The further remarks from Section 6.3.1 apply accordingly.

7. Key Agreement Schemes, Key Transport Schemes and Key Update

Key agreement schemes are used to exchange an encryption key over an insecure channel. It is absolutely essential that these schemes are combined with instance authentication schemes, since otherwise there is no way to decide with which party the key agreement is performed. Data authentication alone is not sufficient here, as an attacker could have recorded a communication carried out in the past in order to use the recorded data for an attack. For this reason, as it has already been the case in Chapter 6, we give in this chapter only general ideas for key agreement schemes and refer to Section A.2 for concrete key agreement schemes that also include instance authentication.

After a successful key agreement, both parties are in possession of a common secret; for methods recommended for the generation of symmetric keys based on this secret, see Section B.1. Essentially, the use of a key derivation function is recommended for this task. In some situations, it may make sense to allow a pre-distributed secret to enter the key derivation function. This can be used, for example, to separate different user groups. Also, additional protection against attacks on the key agreement scheme can be achieved in this way. With regard to a separation of different user groups, it can also be reasonable to take into account further public data specific to both communication partners in the key derivation.

It is recommended to only use key derivation schemes in which communication partners contribute equal shares for the keys to be generated. Both sides should contribute at least 100 bits of entropy. When choosing a key agreement scheme for a particular application, it should also be taken into account whether, in the chosen protocol, one side may have greater control over the key material than the other and whether such an asymmetry may have security implications in the respective application.

In addition to key agreement schemes, key transport schemes, are also of practical importance. In a key transport scheme, secret key data is generated by one party and transported secured to one or more recipients. The generating entity can be a trusted third party or one of the parties involved in the communication. In the latter case, it is recommended that all parties involved only use self-generated keys for the transmission of their own sensitive data. At this point, the recipients have no control over the distributed session keys.

Finally, this chapter also deals with key update schemes. Here, two parties already share a common secret and derive a new key from it at the end of a key change period. This can be achieved either by deriving new session keys from a permanent master key or by an update procedure that generates a new key from the current key and possibly other data. Various factors must be taken into account when determining the lifetime of key material, among them the type of key, the environment of use or the sensitivity of the data to be protected. Further information on this topic can be found, for example, in [99].

Remark 7.1 When cryptographic keys are negotiated with a key agreement scheme or transmitted securely with a key transport scheme, these keys or the cryptographic mechanisms using these keys have at most the same security level as the key agreement or key transport scheme. Since there is a possibility that an attacker records the communication during key agreement or key transport, changed recommendations for key agreement or key transport schemes also have an impact on previously negotiated or transmitted keys. For example, if the key agreement or key transport scheme loses conformance to this Technical Guideline, the keys negotiated or

transferred with it should also no longer be used.

Preliminary Remark: Asymmetric versus Symmetric Key Agreement Schemes Asymmetric key agreement schemes can be used to achieve security properties that cannot be realised using symmetric cryptography alone. For example, both recommended asymmetric key agreement schemes have the property that an adversary who knows all the long-term secrets, if any, of the two parties involved in the communication[1] still cannot determine the key negotiated during an uncompromised protocol execution if he cannot efficiently solve the mathematical problem underlying the asymmetric mechanism used (in the schemes presented here, the Diffie-Hellman problem). In comparison, in symmetric key agreement schemes, at most the security objective *post-compromise security* can be achieved, that means an attacker who knows all the long-term secrets of the two parties involved cannot determine the results of *previously* properly performed key agreements.[2]

7.1. Symmetric Schemes

Key Transport In general, all of the symmetric encryption schemes recommended in Chapter 2 can be used for the transport of session keys. It is recommended to combine an encryption scheme recommended in Chapter 2 with a MAC from section 5.2 (in Encrypt-then-MAC mode) to ensure a manipulation-resistant transmission of the key material.

Key Agreement Key agreement schemes, too, can be realised solely on the basis of symmetric schemes provided that the existence of a common long-term secret can be assumed. Key Establishment Mechanism 5 from [59] represents a suitable scheme. If an implicit key confirmation by possession of the same session keys is not sufficient for the given cryptographic application, it is recommended to extend this protocol by a further key confirmation step. As key derivation function, the mechanism recommended in Section B.1 should be used.

Key Update In some situations it may be necessary to synchronously exchange the keys used in a cryptographic system for all parties involved without a new key exchange or further communication. In this case, key update mechanisms can be used. Assuming that the master key K_t of a cryptosystem is to be replaced at time t via such a mechanism, we recommend to define

$$K_{t+1} \coloneqq \mathrm{KDF}(s, \mathrm{Label}, \mathrm{Context}, L, K_t).$$

Here, KDF denotes a two-step cryptographic key derivation function according to [98, Section 5], and s is the salt value used in the expansion step. The parameters Label and Context enter the expansion step provided in [98] after [90]. Here, Label is a string that identifies the function of the key to be derived and Context contains information about the further protocol context. The parameter L denotes the length of the key K_{t+1} to be derived and also enters into the expansion step.

In this mechanism, it is absolutely essential to ensure that different derivation parameters are used for any derivation of further key material from K_t than those used for the derivation of K_{t+1}. It is recommended to enforce this by using appropriate label values and furthermore to encode in label or context at least also the cryptoperiod t. As an additional measure, it may also make sense to use a new salt value for each key derivation. It is recommended to securely delete K_t immediately after K_{t+1} has been calculated, as well as all intermediate results of the

[1] Here, we primarily mean the long-term secrets that have to be used to secure the connection against man-in-the-middle attacks

[2] *Merkle puzzles* are an exception in this respect in that they constitute a public key key agreement scheme using only symmetric primitives [81]. However, this mechanism is only of academic relevance.

calculation. For further recommendations on the implementation of these schemes, please refer to [98, 90].

7.2. Asymmetric Schemes

In general, all of the asymmetric encryption schemes recommended in Chapter 3 can be used for the transport of session keys.

The recommended asymmetric key exchange schemes are:

• Diffie-Hellman, see [80],
• EC Diffie-Hellman (ECKA-DH), see [35].

Table 7.1: Recommended asymmetric key agreement schemes.

The following algorithms need to be specified:

1.) an algorithm for the definition of the system parameters and

2.) an algorithm for key agreement.

7.2.1. Diffie-Hellman

The security of this mechanism is based on the assumed difficulty of the Diffie-Hellman problem in groups $\mathbb{F}_p$, where p is a prime number.

System Parameters

1.) Randomly choose a prime number p.

2.) Choose an element $g \in \mathbb{F}_p^*$ with $\mathrm{ord}(g)$ prime and $q := \mathrm{ord}(g) \geq 2^{250}$.

The triple (p, g, q) must be authentically exchanged in advance between the parties involved in the communication, where the same system parameters may in principle be used by many users. For the generation of suitable system parameters see Remark 3.7.

Key Agreement

1.) A chooses a random value $x \in \{1, \ldots, q-1\}$ according to the uniform distribution and sends $Q_A := g^x$ to B.

2.) B chooses a random value $y \in \{1, \ldots, q-1\}$ according to the uniform distribution and sends $Q_B := g^y$ to A.

3.) A calculates $(g^y)^x = g^{xy}$.

4.) B calculates $(g^x)^y = g^{xy}$.

The key agreement, too, must be secured by means of strong authentication to prevent man-in-the-middle attacks. The negotiated shared secret is g^{xy}. A mechanism for the subsequent key derivation from this secret is recommended in Section B.1.

Key Length The length of p should be at least 2000 bits, and at least 3000 bits for a period of use beyond 2022. Footnote (a) to Table 3.1 and Remarks 3.2 and 3.3 from Chapter 3 apply accordingly.

Remarks on the Implementation A number of implementation errors are common in the implementation of the Diffie-Hellman protocol. Some of these implementation problems are discussed in [102]. It is recommended that particular attention be paid to section 7 of [102].

7.2.2. EC Diffie-Hellman

The security of this mechanism is based on the assumed difficulty of the Diffie-Hellman problem in elliptic curves.

System Parameters Choose cryptographically strong EC system parameters (p, a, b, P, q, i) according to B.3. Let the elliptic curve thus defined be denoted by C and the cyclic subgroup generated by P by $\mathcal{G}$. The system parameters (p, a, b, P, q, i) must be authentically exchanged in advance between the parties involved in the communication.

Key Agreement

1.) A chooses a random value $x \in \{1, \ldots, q-1\}$ according to the uniform distribution and sends $Q_A \coloneqq x \cdot P$ to B.

2.) B chooses a random value $y \in \{1, \ldots, q-1\}$ according to the uniform distribution and sends $Q_B \coloneqq y \cdot P$ to A.

3.) A calculates $x \cdot Q_B = xy \cdot P$.

4.) B calculates $y \cdot Q_A = xy \cdot P$.

The key agreement, too, must be secured by means of strong authentication. The negotiated secret is $xy \cdot P$. A mechanism for subsequent key derivation from this secret is recommended in Section B.1.

Wherever possible, it is recommended to test on both sides during the exection of the key agreement whether the points Q_A and Q_B have been chosen according to the requirements of the protocol and to abort the protocol if not. If the above protocol is executed correctly, $Q_A \in \mathcal{G}$, $Q_B \in \mathcal{G}$, $Q_A \neq \mathcal{O}$ and $Q_B \neq \mathcal{O}$ should hold. As part of the test of $Q_A, Q_B \in \mathcal{G}$, it should also be explicitly checked whether $Q_A, Q_B \in C$. Further remarks can be found in Section 4.3.2.1 of [35].

Key Length The length of q should be at least 250 bits.

Remarks on the Implementation There are several common implementation errors when implementing a Diffie-Hellman key exchange. Some of these implementation problems are addressed in [102]. It is recommended to observe Section 7 of [102], furthermore the remarks in Section 4.3 of [35] and the AIS46 [33] have to be taken into account.

8. Secret Sharing

In many cases, cryptographic keys have to be stored over a long period of time. This requires in particular that copies of these keys must be made to prevent the loss of the keys. However, as the number of copies grows, so does the likelihood that the secret to be protected is compromised. Therefore, in this chapter, we give a method that allows dividing a secret, such as a cryptographic key K, into n shared secrets $K_1, \ldots, K_n$ in such a way that any $t \leq n$ of these shared secrets are sufficient to reconstruct the secret, but $t-1$ shared secrets provide no information about K. Another application of this scheme is to use a four-eyes principle or, more generally, a t-out-of-n-eyes principle, for example to distribute the password for a cryptographic component among n different users so that at least t users are required to reconstruct the password.

The secret-sharing algorithm presented here was developed by A. Shamir and is therefore also called the Shamir secret-sharing mechanism, see [104]. We assume in the following that the secret to be shared is a key K of bit length r, that is $K = (k_0, \ldots, k_{r-1}) \in \{0,1\}^r$. To compute the shared secrets to n users such that t users can reconstruct the secret K, we proceed as follows:

1.) Choose a prime $p \geq \max(2^r, n+1)$ and set $a_0 \coloneqq \sum_{i=0}^{r-1} k_i \cdot 2^i$.

2.) Independently choose $t-1$ random values $a_1, \ldots, a_{t-1} \in \{0, 1, \ldots, p-1\}$ according to the uniform distribution on $\{0, 1, \ldots, p-1\}$. The values $a_0, a_1, \ldots, a_{t-1}$ define a random polynomial

$$f(x) = \sum_{j=0}^{t-1} a_j x^j$$

over $\mathbb{F}_p$, for which $f(0) = a_0 = \sum_{i=0}^{r-1} k_i \cdot 2^i$ holds.

3.) Calculate the values $K_i \coloneqq f(i)$ for all $i \in \{1, \ldots, n\}$.

Table 8.1: Calculation of the secret shares in Shamir's Secret-Sharing algorithm.

.

The shared secrets K_i are then handed over, along with i, to the i-th user.

Remark 8.1 The basis for the algorithm mentioned in Table 8.1 is the so-called *Lagrange-interpolation-formula*, which allows to determine the coefficients $a_0, \ldots, a_{t-1}$ of an unknown polynomial f of degree $t-1$ from t points $(x_i, f(x_i))$ as follows:

$$f(x) = \sum_{i=1}^{t} \left[f(x_i) \prod_{\substack{1 \leq j \leq t \\ j \neq i}} \frac{x - x_j}{x_i - x_j} \right].$$

In particular, $a_0 = f(0)$ (and thus K) can be calculated in this way from t given points.

In order to reconstruct the secret K from t shared secrets $K_{j_1}, \ldots, K_{j_t}$ (with pairwise different j_l), one calculates $a_0 = \sum_{i=0}^{r-1} k_i \cdot 2^i$ as follows:

1.) For all $j \in \{j_1, \ldots, j_t\}$ calculate the value $c_j = \prod_{\substack{1 \le l \le t \\ j_l \neq j}} \frac{j_l}{j_l - j}$.

2.) Calculate $K = \sum_{l=1}^{t} c_{j_l} K_{j_l}$.

Table 8.2: Reassembly of the shared secret in Shamir's secret-sharing algorithm.

Both when dividing into shared secrets in Table 8.1 and when recombining them in Table 8.2, note, that in each case the calculation is carried out in $\mathbb{F}_p$, that means modulo p.

Remark 8.2 The condition $p \geq \max(2^r, n+1)$ ensures that on the one hand the secret can be represented as an element of $\mathbb{F}_p$ and on the other hand that at least n independent partial secrets can be generated. The algorithm achieves information-theoretic security, which means that it is not possible even for an attacker with unlimited resources to reconstruct the distributed secret without learning t shared secrets or a value derived from the knowledge of t shared secrets in a suitable way.

The security of the scheme therefore does not depend on any further security parameters apart from the stated condition. However, organisational and technical measures must be taken to ensure that an attacker cannot gain knowledge of t shared secrets. Any communication about the shared secrets must therefore be encrypted and authenticated, as far as it is physically possible for an attacker to record or manipulate this communication.

Moreover, information-theoretic security is only given if the a_i for $i > 0$ are chosen truly at random and according to the uniform distribution on $\mathbb{F}_p$. In order to achieve at least complexity theoretical security, a physical random generator of the functionality class PTG.3 or a deterministic random generator of the functionality class DRG.3 or DRG.4 should therefore be used to generate the a_i. The values returned from this random generator must be post-processed to follow the uniform distribution on $\mathbb{F}_p$; suitable methods for this can be found in Section B.4.

9. Random Number Generators

The majority of cryptographic applications require random numbers, for example, to generate cryptographic long-term or ephemeral keys, system parameters or for instance authentication. This applies to symmetric and asymmetric encryption schemes as well as to signature, authentication and padding methods. In general, unsuitable random number generators can substantially weaken strong cryptographic mechanisms, so special care must be taken in cryptographic applications to ensure that suitable random number generators are used. Thus – in contrast to, for example, numerical simulations or experiments, in which reproducibility can play an important role – in the cryptographic context, unpredictability and secrecy of the random numbers and/or the values derived from them are indispensable properties for most applications. Even if an adversary knows long subsequences of random numbers, this should not allow him to determine their predecessors or successors.

Usually, the goal in generating random numbers is to produce output values uniformly distributed on $\{0,1\}^n$. However, in some cases, random numbers with certain other distributions are needed. For this reason, Appendix B contains algorithms that can be used to calculate random values with desired properties (for example, uniformly distributed on $\{0,\ldots,q-1\}$) from the output values of a random number generator.

In the German certification scheme, the AIS 20 [30] (for deterministic random number generators) and AIS 31 [31] (for physical random number generators) are binding. Of central importance is the mathematical-technical annex [29] common to them, which supersedes the predecessor documents [27] and [28]. It defines functionality classes for physical random number generators (PTG.1 - PTG.3), for deterministic random number generators (DRG.1 - DRG.4) and for non-physical non-deterministic random number generators (NTG.1). Furthermore, [29] explains the mathematical background and illustrates the concepts with numerous examples.

In the following sections, the different types of random number generators are discussed in more detail. The main recommendations for the use of random number generators in general cryptographic applications can be summarised as follows:

- When using a physical random number generator, it is generally recommended to use a PTG.3 generator. This is especially true for the generation of ephemeral keys when computing digital signatures and Diffie-Hellman based key negotiation. In cases where the use of a certified cryptographic component is required for random number generation, this recommendation only applies if correspondingly certified components are available. Otherwise, a PTG.3 generator can usually be constructed by cryptographic post-processing of the output of a PTG.2 generator, implemented in software and compatible with the requirements of the PTG.3 functionality class.

- For some specific cryptographic applications, PTG.2 generators are also sufficient, for example when generating symmetric session keys or when generating a seed for a strong deterministic random number generator. Random numbers from PTG.2-compliant random number generators have high entropy, but may have some biases and/or dependencies. They may be used in some circumstances if the resulting advantage to an adversary is demonstrably small. In general, however, the direct use of PTG.2 random number generators is discouraged. This applies in particular to applications in which the existence of even relatively minor biases in the distribution of the generated random numbers can

lead to exploitable weaknesses, such as in the generation of nonces in DSA-like signature procedures.

- When using a deterministic random number generator, it is recommended to use a DRG.3 or a DRG.4 generator whose seed is generated from a physical random source of class PTG.2 or PTG.3. If no such random source is available, the use of a non-physical, non-deterministic random number generator may also be considered in some circumstances. For example, a DRG.3 generator can also be seeded with an NTG.1 generator, for further details please refer to Sections 9.3 and 9.5 .

- In general, PTG.3 and DRG.4 generators have the advantage of an improved resistance to side-channel and fault attacks compared to PTG.2 and DRG.3 generators. In the case of a PTG.3 generator, the permanent inflow of large amounts of entropy into the internal state means that possible side-channel attacks against cryptographic post-processing are made considerably more difficult, as an adversary can combine information about the internal state at two consecutive points in time t and $t+1$ only with great difficulty.

- In addition to the risk of long-term compromise through side-channel and fault attacks, DRG.3 random number generators have an increased residual risk of long-term conceivable cryptanalytic compromise compared to DRG.4 and PTG.3 generators if the random number generator produces large amounts of key material worthy of long-term protection from a single seed value. In comparison, when using PTG.3 or DRG.4 random number generators, side-channel and fault attacks are also relevant, but only lead to the compromise of relatively few generated random.

- The requirements on the min-entropy of the seed of a deterministic random number generator increase accordingly if a security level of more than 100 bits is aimed at for a cryptographic system as a whole. In the general case, a system security of n bits requires a min-entropy of the RNG seed of n bits.

- For both physical and deterministic random number generators, resistance to high attack potential should be demonstrated in the respective application context.

9.1. Physical Random Number Generators

Physical random number generators use dedicated hardware (usually an electronic circuit), to generate „true“ randomness, that means unpredictable random numbers. This is usually done by exploiting the unpredictable behaviour of simple electrical circuits, as can be caused by various forms of noise in the circuits. In the end, the entropy of the signal is physically usually based on quantum effects or on the amplification of environmental influences in a chaotic system, where the influences cannot be controlled or separately measured. An adversary should have only a negligible (ideally no) advantage over blindly guessing the random numbers even with knowledge of partial sequences of random numbers as well as the exact knowledge of the random number generator including the physical environmental conditions at the time of the generation of previous or subsequent random numbers. Deterministic post-processing of the „raw noise data“ (usually digitised noise signals) is often necessary to eliminate any biases or dependencies that may be present.

When using a physical random number generator, it is generally recommended to use a PTG.3 generator in the sense of AIS 31 (compare [29, Chapter 4]). This applies in particular to applications in which an adversary can, at least in principle, combine information about different random numbers. If an implementation of the random number generator in a certified cryptographic component is required, the recommendation to use a PTG.3 generator only applies if suitable certified components exist.

It is possible to construct a PTG.3 generator from a PTG.2 generator by cryptographically post-processing the output of the PTG.2 generator in a suitable manner. This post-processing can usually be implemented in software. The exact requirements for post-processing can be found in [29]. Roughly speaking, the post-processing must implement a DRG.3-compatible deterministic random number generator and at least as much new entropy must always be added to the internal state of the random number generator by a random number generator of class PTG.2 as is requested by the cryptographic application.

In short, PTG.2 or PTG.3 compliant random number generators must fulfil the following properties:

- The statistical properties of the random numbers can be described sufficiently well by a stochastic model. Based on this stochastic model, the entropy of the random numbers can be reliably estimated.
- The average entropy increase per random bit is above a given minimum limit (close to 1).
- The digitised noise signals are subjected to statistical tests online, which are suitable to detect unacceptable statistical defects or degradation of statistical properties within a reasonable period of time.
- A total failure of the noise source is de facto detected immediately. No random numbers generated after a total failure of the noise source must be output.
- The detection of a total failure of the noise source or unacceptable statistical defects of the random numbers leads to a noise alarm. A noise alarm is followed by a defined, appropriate response (for example, shutting down the noise source).
- (Only PTG.3-compliant random number generators) A (possibly additional) strong cryptographic post-processing ensures that even in the case of an unnoticed total failure of the noise source, the security level of a DRG.3-compliant deterministic random number generator is still assured.

Hybrid random number generators combine security properties of deterministic and physical random number generators. In addition to a strong noise source, hybrid physical random number generators of functionality class PTG.3 have a strong cryptographic post-processing with memory. This is typically realised by a cryptographic post-processing of the random numbers of a PTG.2-compliant random number generator in an appropriate manner.

The development and security-critical assessment of physical random number generators require comprehensive experience in this field and it is recommended to seek advice of experts at an early stage.

9.2. Deterministic Random Number Generators

Deterministic random number generators (also known as pseudorandom number generators) can compute a pseudorandom bit sequence of practically any length from a fixed-length random value called a *seed*. Publicly known parameters can also be included in the computation. For this purpose, the inner state of the pseudorandom number generator is first initialised with the seed. In each step, the internal state is then renewed, and a random number (usually a bit sequence of fixed length) is derived from the internal state and output. Hybrid deterministic random number generators refresh the inner state from time to time with „true“ random values (reseed/seed update). This can be initiated in different ways, for example regularly or on request of the application. The inner state of a deterministic random number generator must be reliably protected against readout and manipulation. If a deterministic random number generator is

used, then it is recommended to use a DRG.3 or DRG.4-compliant random number generator against the attack potential „high“ in the sense of AIS 20 (see [29]).

When using random number generators of the functionality class DRG.3, a steady inflow of fresh entropy into the internal state is desirable, even if it is not sufficiently regular or of high enough quality to achieve DRG.4-compliance for the overall design. Roughly speaking, DRG.3 conformity means:

- It is practically impossible for an adversary to calculate predecessors or successors of random numbers to a known subsequence of random numbers or to guess them with significantly higher probability than would be possible without knowledge of this subsequence.
- It is practically impossible for an adversary to calculate previously output random numbers based on knowledge of an internal state or to guess them with significantly higher probability than would be possible without knowledge of the internal stat state.

For DRG.4-compliance, even if an adversary knows the current internal state, it is not practically possible for him to compute random numbers that are generated after the next reseed/seed update or to guess them with significantly higher probability than would be possible without knowledge of the inner state.[1] DRG.4 generators also have certain advantages over DRG.3-compliant random number generators in terms of implementation attacks.

9.3. Non-Physical Non-Deterministic Random Number Generators

For many cryptographic applications, for example in the field of e-business or e-government, neither a physical nor a deterministic random number generator is available, since these applications are generally run on computers without certified cryptographic hardware. Instead, non-physical non-deterministic random number generators (NPTRNG) are generally used, either directly or to seed a strong deterministic random number generator. A well-known example of a non-physical non-deterministic random number generator is the Linux RNG (device file `/dev/random`), which is analysed in detail in the study [5].

Like physical random number generators, non-physical non-deterministic random number generators generate „true“ random numbers and rely on security in the information-theoretic sense through sufficient entropy. However, they do not use dedicated hardware for this, but system resources (system time, RAM contents, etc.) and/or user interaction (for example, keystrokes or mouse movements). Non-physical non-deterministic random number generators are usually used on systems that are not specifically designed for cryptographic applications, for example, commercially available PCs, laptops or smartphones.

A typical approach for generating random numbers using non-physical non-deterministic random number generators is as follows: First, a long bit string of „random data“ (more precisely: of non-deterministic data) is generated, where the entropy per bit is usually rather low. This bit string is mixed with an internal state and random numbers are then calculated from the internal state and output afterwards.

In the mathematical-technical annex [29], a functionality class for such random number generators (NTG.1) is defined. For NTG.1 random number generators, it is roughly speaking required that the amount of entropy collected during operation can be reliably estimated and that the output data have a Shannon entropy of > 0.997 bits per output bit.

This means, among other things:

[1] Significantly higher probability here refers to a probability at least higher than the probability of guessing the true random values generated for the seed update. For each seed update, at least 100 bits of min-entropy must be generated.

- The entropy of the internal state is estimated. If a random number is output, the entropy counter is reduced accordingly.
- Random numbers may only be output if the value of the entropy counter is high enough.
- It is practically impossible for an adversary to calculate previously output random numbers based on the knowledge of the internal state and the random bit strings previously used for seed updates or to guess them with significantly higher probability than would be possible without knowledge of the state and bit strings.

It is crucial for NPTRNG that the entropy sources used by the random number generator cannot be manipulated by an adversary in the sense of entropy reduction or become predictable if the adversary has precise information about the execution environment. This requirement is not a matter of course even when using an actually good NPTRNG. An example of a critical situation in this respect is the use of virtualisation solutions [103]. In this case, the output of an NPTRNG can, in extreme cases, be completely predicted if the system is started twice from the same system image and all entropy sources of the virtual system are controlled by the host computer.

If an NPTRNG is to be used as the sole or most important random source for a system intended to process sensitive data, it is strongly recommended to always consult an expert.

9.4. Various Aspects

Hybrid random number generators combine security properties of deterministic and physical random number generators. The security of a hybrid deterministic random number generator of functionality class DRG.4 is primarily based on the complexity of the deterministic part, which belongs to class DRG.3. During the use of the random number generator, new randomness is also added again and again. This can be done, for example, at regular intervals or at the request of an application.

In addition to a strong noise source, hybrid physical random number generators of functionality class PTG.3 have a strong cryptographic post-processing with memory. Compared to PTG.2-compliant random number generators, the PTG.3 functionality class also offers the advantage that the random numbers have neither biases nor exploitable dependencies. Especially for applications in which a potential adversary can, at least in principle, combine information about many random numbers (for example, ephemeral keys), a physical random number generator of functionality class PTG.3 should be used.

The derivation of signature keys, ephemeral keys and prime numbers (for RSA) or the like from the generated random numbers has to be done with suitable algorithms (for elliptic curves compare [33, Sections 5.2 and 5.5.1]). Roughly speaking, a potential adversary should have as little information as possible about the derived values (to be kept secret). Ideally, all values within the respective permissible range of values occur with the same probability, and different random numbers should at least have no practically exploitable correlations. As explained in [29], the generation of secret signature keys, ephemeral keys and prime numbers can also be the target of side-channel attacks, just like signature algorithms (see for example [49, 33]).

9.5. Seed Generation for Deterministic Random Number Generators

For the initialisation of a deterministic random number generator, a seed with sufficiently high entropy is required. This seed should be generated with a physical random number generator of the functionality classes PTG.2 or PTG.3. On PCs, a physical random number generator

is usually not available, or at least such a random number generator has not been subjected to thorough manufacturer-independent certification. In such cases, the use of a non-physical non-deterministic random number generator is recommended; NTG.1-compliant random number generators (high attack potential) are suitable for this purpose. Currently, there are no NTG.1-certified random number generators. Therefore, we give below suitable methods for seed generation for the two most important PC operating systems.

However, the use of the methods for seed generation recommended in the following two subsections can only be viewed as secure if the computer is under the user's complete control and no third-party components have direct access to the entire internal state of the computer, as may be the case, for example, if the entire operating system runs in a virtual environment. This means for example in particular that the existence of viruses or Trojan horses on this computer can be ruled out. Users must be informed about these risks.

9.5.1. GNU/Linux

The following mechanism is recommended for seed generation under the GNU/Linux operating system:

Reading of data from the device file `/dev/random`.

Table 9.1: Recommended method for seed generation under GNU/Linux.

Remark 9.1 The randomness provided by the device file `/dev/random` has so far only been reviewed by the BSI for certain kernel versions and found to be suitable when used in PC-like systems. The Linux RNG is thereby assessed by the present Technical Guideline as generally suitable for general cryptographic applications if the requirements of the functionality class DRG.3 or NTG.1 according to [29] are fulfilled. However, since the underlying mechanisms differ considerably depending on the kernel version used and the available random sources depend on the exact system environment, an expert should always be consulted if `/dev/random` is to be used as the main random source in a new system to be developed. A cryptographic evaluation of `/dev/random` in different Linux kernel versions can be found in the BSI study [5]. A cross-check of the security properties of the Linux random number generator in different Linux kernel versions with the functionality classes of AIS 20 and AIS 31 respectively is given in the kernel overviews included there.

Remark 9.2 The use of `/dev/urandom` can be problematic [52], as it does not check whether a sufficient amount of system data has been collected for cryptographic purposes at initialisation of the random number generator. On the other hand, `/dev/random` blocks in some kernel versions if the internal entropy estimator falls below a specified bound. This can slow down random number generation a lot, leading to usability problems.

Remark 9.3 In principle, `/dev/random` can be used not only to seed a pseudorandom generator, but also to generate cryptographic keys directly.

9.5.2. Windows

In contrast to GNU/Linux operating systems, there is currently no function for the operating systems of the Windows family that guarantees adequate high entropy and has been examined by the BSI. For the generation of secure seeds, several sources of entropy should be combined in an appropriate manner. For example, in Windows 10, to generate a seed value of at least 120 bits of entropy, the following method may be considerable:

1.) Reading of 128 bits of random data into a 128-bit buffer S_1 from the Windows API function `BCryptGenRandom()`.

2.) Obtaining a bit string S_2 with at least 120 bits of entropy from a *different source*. Here, for example, the following can be considered:

- Evaluation of the time intervals between successive keystrokes of the user: If these can be demonstrably recorded with a precision of one millisecond, about three bits of entropy per keystroke can be conservatively assumed for this. In order to estimate the temporal resolution of the measured time intervals, the entire processing chain must be examined for entropy-limiting factors. For example, it is possible that the accuracy of the internal clock gives one resolution limit, the polling frequency of the keyboard another, and the time interval within which the used system timers are being updated yet another. It is recommended to measure the distribution of the keyboard stroke times in practical tests beforehand and to examine them for anomalies. The sequence of the recorded timings of a sufficiently large number of keyboard events can then be encoded into a binary string B. Subsequently, one sets $S_2 := \mathrm{SHA256}(B)$ and the recorded data on keyboard stroke times (and other data collected in the process) are cleared from working memory by overwriting with zeros.
- User-initiated events: The times $T_1, T_2, T_3, T_4, T_5, T_6$ of six events initiated by the user are recorded using the Windows API function `QueryPerformanceCounter()`. This usually has an accuracy of at least the order of a microsecond. One can, under the conditions,

  (i) that each T_i cannot be estimated more precisely than to one second even if T_j is known to the adversary for all $j \neq i$,

  (ii) that even if T_j is known to the adversary for all $j \neq i$, the value of T_i cannot be constrained by other considerations (for example, to the polling frequency of the keyboard) to less than 2^{20} possibilities if any interval of one second in length containing T_i is given,

  assume that the bit string $T := T_1||T_2||T_3||T_4||T_5||T_6$ contains about 120 bits of entropy from the adversary's point of view. As in the previous example, one sets $S_2 := \mathrm{SHA256}(T)$ and clears T from working memory.

  It is not always easy to meet the requirements for independence and unpredictability of user-initiated events. The problem here is that the time at which the software requests the user to initiate an event may be tightly predictable if the timing of an earlier event is known. The time that elapses between the request for an input and the user input itself might also be more accurately predictable than in the range of seconds. The fulfilment of the prerequisites and the plausibility of such entropy estimates must always be examined in the each particular case at hand.
- In a similar way, mouse movements of the user can also be used to gather entropy. The entropy contained in mouse movements cannot be estimated precisely without further analysis. Therefore, a case-by-case analysis is always required, taking into account the type and number of events recorded (pointer positions, and additionally time measurements if necessary), so that it can be ensured that the measurements collected cannot be compressed without loss to a data set of less than 120 bits in size. One then defines S_2 again by a SHA2 hash over the recorded mouse events.

3.) In all cases, a seed value S for a suitable pseudorandom generator can then be derived by setting $S := \mathrm{SHA256}(S_1||S_2)$. Ideally, as many independent entropy sources $S_1, \ldots, S_n$ as possible are used to achieve a desired level of security.

Remark 9.4 There is nothing known to the BSI indicating that in the above example a 128-bit value obtained from `BCryptGenRandom()` does not already contain approximately 128 bits of entropy. However, the exact operation of `BCryptGenRandom()` is not described in detail in publicly available vendor documents, nor has the function been intensively studied by parties independent of the vendor, as is the case, for example, for the random number generator integrated into the Linux kernel. Therefore, combining randomness from `BCryptGenRandom()` with output from other entropy sources is recommended as a basic precaution.

Appendix A.

Application of Cryptographic Mechanisms

The mechanisms explained in the previous chapters often have to be combined in order to ensure the protection of sensitive data. In particular, sensitive data to be transmitted should not only be encrypted but also authenticated in order to enable a recipient to detect any changes.

Moreover, a key agreement must always be accompanied by an instance authentication and an authentication of all messages transmitted during the key agreement, so that both parties can be sure who they are communicating with. Otherwise, the communication can be compromised by a so-called man-in-the-middle attack. Depending on the application, in addition to man-in-the-middle attacks, other types of attacks on the authenticity of message transmission (for example, replay attacks) can also threaten the security of an information-processing system without instance authentication or without data authentication. Therefore, in this chapter adequate mechanisms for both encryption with data authentication and authenticated key agreement are provided.

A.1. Encryption Methods with Data Authentication (Secure Messaging)

In principle, all mechanisms recommended in Chapter 2 or Section 5.2 can be used for the combination of encryption and data authentication.

The following two aspects must be observed:

- Encrypted data must always be transmitted authenticated. In addition, it is possible to transmit non-confidential data authenticated but unencrypted. All other data of the same data transmission is *not* authenticated.
- Encryption and authentication keys must be different and should not be derivable from each other.

Remark A.1 It is possible to derive encryption and authentication keys from a shared key; this does not contradict the second aspect above. Recommended mechanisms are summarised in Section B.1.

Remark A.2 For the authenticated transmission of encrypted data, the use of a MAC in Encrypt-then-MAC mode is recommended.

Remark A.3 If the security objective of non-repudiation of the plaintext is also sought in a transmission of encrypted data, the plaintext should be secured by a digital signature. In this case, the plaintext is thus first signed, then encrypted, and finally the encrypted transmission is protected by a MAC against modification on the transmission path. Moreover, a signature on the ciphertext can be reasonable if in addition the encrypted message should be non-repudiable or only the sender (and not the legitimate recipient) should be able to change the ciphertext. In general, however, the signer cannot meaningfully check the ciphertext before signing it.

A.2. Key Agreement with Instance Authentication

As already mentioned, a key agreement must always be combined with an instance authentication. After some general preliminary remarks, we provide schemes based either entirely on symmetric algorithms or entirely on asymmetric algorithms.

A.2.1. Preliminary Remarks

Objectives The objective of a key exchange scheme with instance authentication is that the parties involved share a common secret afterwards and are sure with whom they share it at the end of the protocol execution. For the derivation of symmetric keys for encryption and data authentication schemes from this secret, see Section B.1.

Requirements on the Environment Symmetric schemes for an authenticated key exchange always assume the existence of pre-distributed secrets. In the case of asymmetric schemes it is usually assumed that a public key infrastructure that is able to reliably bind keys to identities and to authenticate the origin of a key through appropriate certificates exists. Further it is assumed that the root certificates of the PKI have been made known to all parties involved via reliable channels and that all parties are able to check the validity of all relevant certificates at any time.

For the practical implementation of the schemes presented, the following two conditions must be fulfilled:

- The random values used for the authentication have to be different with high probabilityeach time the protocol is executed. This can be achieved, for example, by choosing each time a random value with respect to the uniform distribution on $\{0,1\}^{100}$.
- The random values used for key agreement must at least reach an entropy that corresponds to the desired key lengths of the keys to be to be agreed upon. It is assumed at this point that only symmetric keys are negotiated. In addition, each party involved in the key agreement should contribute at least 100 bits of min-entropy to the key to be negotiated.

A.2.2. Symmetric Schemes

In principle, any scheme for instance authentication from Section 6.1 can be combined with any scheme for key agreement from Section 7.1. The combination must be done in such a way that the exchanged keys are actually authenticated and thus in particular man-in-the-middle attacks can be excluded. The following mechanism is recommended for this application:

Key Establishment Mechanism 5 from [59].

Table A.1: Recommended Symmetric Scheme for Key Agreement with Instance Authentication.

Remark A.4 Any of the authenticated encryption schemes recommended in this Technical Guideline may be used as encryption methods in Key Establishment Mechanism 5 from [59] (see Section A.1).

A.2.3. Asymmetric Schemes

Analogous to symmetric schemes, any scheme for instance authentication from Section 6.2 can be combined with any mechanism for key agreement from Section 7.2. However, in order to prevent errors in self-designed protocols the key agreement schemes listed in Table A.2 are recommended for key agreement with instance authentication based on asymmetric schemes.

All recommended schemes require the existence of a mechanism for authentic distribution of public keys as a precondition. This mechanism must have the following properties:

- The public key generated by a user must be reliably bound to the user's identity.
- The associated private key should be reliably bound to the identity of the user (it should not be possible for a user to register a public key under his identity to which he cannot use the associated private key).

There are several ways to achieve this. An authentic key distribution can be achieved by means of a PKI. The requirement that the owners of all certificates issued by the PKI should actually be users of the associated private keys can be verified by the PKI performing one of the instance authentication protocols described in Section 6.2 with the applicant using his public key before issuing the certificate.

If the PKI does not perform such a check, it is recommended to add a key confirmation step to the schemes recommended below, in which it is verified that both parties have determined the same shared secret K and in which this secret is bound to the identities of the two parties. For key confirmation, the scheme described in [96, Section 5.6.2] is recommended. The second recommended mechanism (KAS2-bilateral-confirmation according to [96]) already includes this step.

- Elliptic Curve Key Agreement of ElGamal Type (ECKA-EG), see [35],
- Instance Authentication with RSA and Key Agreement with RSA, see KAS2-bilateral-confirmation after [96, section 8.3.3.4],
- MTI(A0), see [63, Annex D.7].

Table A.2: Recommended asymmetric schemes for key agreement with instance authentication.

Remark A.5 In order to comply with the present Technical Guideline, care must be taken in the specific implementation of the protocols that only that only the cryptographic components recommended in this recommended are used.

Remark A.6 In the case of the ECKA-EG scheme, no mutual authentication takes place. Here, one party merely proves to the other that it is in possession of a private key, and even this is done only implicitly, through the possession of the negotiated secret after the execution of the protocol.

Appendix B.
Additional Functions and Algorithms

For some of the cryptographic methods recommended in this Technical Guideline, additional functions and algorithms are required, for example, to generate system parameters or to derive symmetric keys from the output obtained by random number generators or key agreement schemes. These functions and algorithms must be carefully chosen in order to achieve the level of security required in this Technical Guideline and to prevent cryptanalytic attacks.

B.1. Key Derivation

B.1.1. Key Derivation after Key Exchange

After a key agreement, both parties hold a shared secret. Im many applications, several symmetric keys, for example for encryption and data authentication, have to be derived from this secret (see also Remark A.1), which can be realised with the help of a key derivation function. In addition, the following objectives can also be achieved by using a key derivation function:

- Binding of key material to protocol data (for example name of the sender, name of the recipient,...) by using the protocol data in the key derivation function.
- Derivation of session keys or keys for different purposes from a master key also in purely symmetric cryptosystems.
- Post-processing of random data to remove statistical biases in cryptographic key generation.

The following method is recommended for all applications of key derivation functions:

Key Derivation through Extraction-then-Expansion according to [98, Section 5].

Table B.1: Recommended method for key derivation.

In the context of this Technical Guideline, it is recommended to use one of the MACs recommended in Section 5.2 as MAC function in the mentioned mechanism.

B.1.2. Password-Based Key Derivation

In password-based key derivation, a cryptographic key (such as for hard disk encryption) is derived directly from a password entered by a user. When using user-generated passwords, a security level of 120 bits is usually unreachable due to the lack of entropy in human-generated passwords.

In such situations, this Technical Guideline primarily recommends to use a MAC with a secret key used only for this purpose to derive the required secret from the password entered by the

user. The MAC should be computed on a cryptographically secure hardware element that is locally available in the system that checks the password. As MAC, a CMAC or HMAC with at least 128 bits key length should be used and the password should be combined with a salt value of at least 32 bits length. If authentication or key derivation fails, the hardware component should implement a delayed response in order to prevent local brute force attacks. In this case, the quality of the passwords must meet the requirements from Section 6.3.1, whereby offline attacks can be considered as inapplicable.

If the use of a a cryptographic hardware token for password-based key derivation is not possible, the hash function `Argon2id` should be used. The security parameters of `Argon2id` and the requirements for the passwords depend on the application scenario and should be discussed with an expert.

B.2. Generation of Unpredictable Initialisation Vectors

As already mentioned in Section 2.1.2, initialisation vectors for symmetric encryption encryption schemes that use the Cipher Block Chaining (CBC) mode of operation. must be unpredictable. This does not mean that the initialisation vectors must be kept confidential, but only that a possible attacker must not be able to practically guess initialisation vectors that will be used in the future. Furthermore, the attacker must not be able to influence the choice of initialisation vectors either.

This Technical Guideline recommends the following two mechanisms for generating unpredictable initialisation vectors, where n is the block size of the block cipher used: with the block cipher and key currently in use and use the ciphertext as an initialisation vector.

Random Initialisation Vectors: Generation of a random bit sequence of length n using a suitable random number generator (see Chapter 9) and using this bit sequence as an initialisation vector.

Encrypted Initialisation Vectors: Use of a deterministic mechanism for the generation of pre-initialisation vectors (for example a counter). Encryption of the pre-initialisation vector with the block cipher and key currently in use and use of the ciphertext as the initialisation vector.

Table B.2: Recommended methods for the generation of unpredictable initialisation vectors.

In the second method, it has to be ensured that the pre-initialisation vectors are not repeated during the lifetime of the system. If a counter is used as a pre-initialisation vector, this means that counter overflows must not occur during the entire lifetime of the system.

B.3. Generation of EC System Parameters

The security of asymmetric mechanisms based on elliptic curves is derived from the assumed difficulty of computing discrete logarithms in these groups.

The following ingredients are needed to define EC system parameters:

1.) Prime number p,

2.) Curve parameters $a, b \in \mathbb{F}_p$ with $4a^3 + 27b^2 \neq 0$, which define an elliptic curve

$$E = \{(x, y) \in \mathbb{F}_p \times \mathbb{F}_p;\ y^2 = x^3 + ax + b\} \cup \{\mathcal{O}_E\},$$

3.) Base point P on $E(\mathbb{F}_p)$.

The *EC system parameters* are then given by the values (p, a, b, P, q, i), where $q := \mathrm{ord}(P)$ denotes the order of the base point P in $E(\mathbb{F}_p)$ and $i := \mathrm{Card}(E(\mathbb{F}_p)/q)$ is the is the so-called *cofactor*.

Not all EC system parameters are suitable for the asymmetric, elliptic curve-based schemes recommended in this Technical Guideline, in the sense that for some parameter constellations the discrete logarithm problem is efficiently solvable in the groups generated by these elliptic curves. Besides a sufficient bit length of q, the following conditions must also be fulfilled, see [74] for more information:

- The order $q = \mathrm{ord}(P)$ of the base point P is a prime number different from p.
- $p^r \neq 1 \bmod q$ for all $1 \leq r \leq 10^4$.
- The class number of the maximal order belonging to the endomorphism ring of E is at least 10^7.

EC system parameters that satisfy the above conditions are also referred to as *cryptographically strong*.

Remark B.1 It is recommended not to generate the EC system parameters on one's own, but instead to use standardised values that are provided by a trustworthy authority.

The system parameters listed in Table B.3 are recommended:

- brainpoolP256r1, see [74],
- brainpoolP320r1, see [74],
- brainpoolP384r1, see [74],
- brainpoolP512r1, see [74].

Table B.3: Recommended EC system parameters for asymmetric schemes that are based on elliptic curves.

B.4. Generation of Random Numbers for Probabilistic Asymmetric Schemes

This Technical Guideline discusses several asymmetric mechanisms that require random numbers $k \in \{1, \ldots, q-1\}$ (for example, as ephemeral keys), where q is usually not a power of 2. Already in the Remarks 3.5, 3.6, 5.6 and 5.8 it was pointed out that k should be chosen to be (at least nearly) uniformly distributed if possible. In contrast, the random number generators presented in Chapter 9 generate uniformly distributed random numbers on $\{0, 1, \ldots, 2^n - 1\}$ („random n-bit strings“). The task is thus to derive (at least nearly) uniformly distributed random numbers on $\{0, 1, \ldots, q\}$ from these random numbers.

In Algorithms B.1 and B.2 two methods are presented that achieve this objective, where $n \in \mathbb{N}$ is chosen such that $2^{n-1} \leq q < 2^n - 1$ holds, in other words q has bit length n.

Algorithmus B.1: Method 1 for computing random values on $\{0, \ldots, q-1\}$.

Input: $n \in \mathbb{N}$ with $2^{n-1} \leq q < 2^n - 1$
Output: $k \in \{0, 1, \ldots, q-1\}$ equally distributed
1: Choose $k \in \{0, 1, \ldots, 2^n - 1\}$ equally distributed.
2: **while** $k \geq q$ **do**
3: Choose $k \in \{0, 1, \ldots, 2^n - 1\}$ equally distributed.
4: **end while**

Algorithmus B.2: Method 2 for computing random values on $\{0, \ldots, q-1\}$.

Input: $n \in \mathbb{N}$ with $2^{n-1} \leq q < 2^n - 1$
Output: $k \in \{0, 1, \ldots, q-1\}$ (almost) equally distributed.
1: Choose $k' \in \{0, 1, \ldots, 2^{n+64} - 1\}$ equally distributed.
2: Set $k = k' \bmod q$.

Remark B.2 (i) Method 1 in Algorithm B.1 converts a uniform distribution on $\{0, \ldots, 2^n - 1\}$ into a uniform distribution on $\{0, \ldots, q-1\}$. More precisely, Method 1 yields the conditional distribution on $\{0, \ldots, q-1\} \subset \{0, \ldots, 2^n - 1\}$. In contrast, Method 2 in Algorithm B.2 does not produce a (perfect) uniform distribution on $\{0, \ldots, q-1\}$ even for ideal random number generators with values in $\{0, \ldots, 2^n - 1\}$. However, the deviations are so small that, according to current knowledge, they cannot be exploited by an attacker.

(ii) The second method has the advantage that any existing skewnesses on $\{0, \ldots, 2^n - 1\}$ are generally reduced. Therefore, only this method is recommended for PTG.2-compliant random number generators. However, it should be noted that the direct use of PTG.2 generators is no longer recommended.

(iii) The disadvantage of Method 1 is that the number of iterations (and thus the runtime) is not constant. For some applications, however, it may be necessary to guarantee an upper bound on the runtime. At this point it should be noted that the probability that a random number uniformly distributed on $k \in \{0, 1, \ldots, 2^n - 1\}$ is less than q is greater than $q/2^n \geq 2^{n-1}/2^n = 1/2$.

B.5. Generation of Prime Numbers

B.5.1. Preliminary Remarks

When defining the system parameters for RSA-based asymmetric schemes, two prime numbers p and q must be chosen. For the security of the schemes, it is necessary that these prime are kept secret. This requires, in particular, that p and q are chosen randomly. With regard to the usability of an application in which RSA-based schemes are used, it is also important that the prime number generation can be performed efficiently. It should be noted that proprietary speed optimisations in key generation can cause significant cryptographic weaknesses, see for example [100]. It is therefore strongly recommended to use mechanisms that are publicly known and have been examined with regard to their security.

Routines for the generation of random prime numbers are also needed for the generation of system parameters for ECC- or finite field arithmetic-based cryptosystems without special properties. The requirements for these primes differ from those for the RSA mechanism in that primes need not be kept secret, but instead it may be relevant that their generation is *verifiable random*. Further details and references on this topic can be found in Section B.3.

B.5.2. Methods for Generating Prime Numbers

Three mechanisms are acceptable for generating random primes lying in a given interval $[a, b] \cap \mathbb{N}$, which can be briefly summarised as follows:

1.) Uniform generation of random primes by rejection sampling;

2.) Uniform generation of an invertible residue class r with respect to $B\#$, where $B\#$ is the *primorial* of B, that means the product of all primes smaller than B, followed by the choice of a prime of suitable size with residue r mod $B\#$ by rejection sampling;

3.) Generation of a random number s of suitable size which is coprime to $B\#$ and search for the next prime in the arithmetic sequence given by $s, s + B\#, s + 2 \cdot B\#, \ldots$.

The first two methods are equally recommended; the third method produces certain statistical biases in the distribution of the generated primes, which are generally undesirable. However, it is widely used in practice (see, for example,[108, Table 1]) and there is currently no evidence that the induced statistical biases can be used for attacks. Therefore, this method is accepted as a legacy method in this Technical Guideline.

The following tables provide a more detailed description of the three methods supported by this Technical Guideline:

Algorithmus B.3: Recommended Method 1 for prime number generation by rejection sampling.

Input: Interval $I := [a, b] \cap \mathbb{N}$
Output: $p \in I$ prime

1: Choose $p \in I$ odd and uniformly distributed on I.
2: **while** p composite **do**
3: Choose $p \in I$ odd and uniformly distributed on I.
4: **end while**

Algorithmus B.4: Recommended Method 2 for prime number generation by efficiency-optimised rejection sampling.

Input: Interval $I := [a, b] \cap \mathbb{N}$, $B \in \mathbb{N}$ with $S := B\# \ll b - a$
Output: $p \in I$ prim

1: Choose r in $\mathbb{Z}/S$ uniformly distributed (equivalently, choose $r < S$ randomly with $\gcd(r, S) = 1$).
2: **while** p composite **do**
3: Choose $k \in \mathbb{N}$ randomly such that $p := kS + r \in I$ (equivalently, choose k equally distributed on $[\lceil (a - r)/S \rceil, \lfloor (b - r)/S \rfloor]$).
4: **end while**

Algorithmus B.5: Legacy Method for prime number generation by incremental search.

Input: Interval $I \coloneqq [a, b] \cap \mathbb{N}$, $B \in \mathbb{N}$ with $S \coloneqq B\# \ll b - a$

Output: $p \in I$ prim

1: **repeat**
2: Choose r in $\mathbb{Z}/S$ uniformly distributed (equivalently, choose $r < S$ randomly with $\gcd(r, S) = 1$).
3: Choose $k \in \mathbb{N}$ randomly such that $p \coloneqq kS + r \in I$ (equivalently: choose k equally distributed on $[\lceil (a - r)/S \rceil, \lfloor (b - r)/S \rfloor]$).
4: **while** p composite, $p \in I$ **do**
5: $p \leftarrow p + S$
6: **end while**
7: **until** p prime

For reasons of efficiency, a probabilistic primality test is usually used as a primality test in the algorithms described above. The following algorithm is recommended in this Technical Guideline:

Miller-Rabin, see [80, Algorithmus 4.24].

Table B.4: Recommended probabilistic primality test.

Remark B.3 (Miller-Rabin Algorithm) The Miller-Rabin algorithm requires, in addition to the number p to be examined, a random value $x \in \{2, 3, \ldots, p - 2\}$, the so-called basis. If x is uniformly distributed on $\{2, 3, \ldots, p - 2\}$, the probability that p is although the Miller-Rabin algorithm outputs that p is a prime, is at most $1/4$.

Worst Case: To bound the probability that a fixed number p is output as a prime number by means of the Miller-Rabin algorithm even though it is composite, the algorithm must be repeated 50 times, each time with bases $x_1, \ldots, x_{50} \in \{2, 3, \ldots, p - 2\}$ chosen independently of each other with respect to the uniform distribution, see further Section B.4 for recommended mechanisms for computing uniformly distributed random numbers on $\{2, 3, \ldots, p - 2\}$.

Average Case: In order to test a randomly with respect to the uniform distribution chosen odd number number $p \in [2^{b-1}, 2^b - 1]$ with the desired certainty for its prime property, far fewer iterations of the Miller-Rabin algorithm are sufficient than the estimate given above would suggest, compare [43], [92, Appendix F] and [61, Annex A]. For example, for $b = 1024$, only four iterations are needed to exclude, with a remaining error probability of 2^{-109}, that p is is composite, although the Miller-Rabin algorithm identifies p as a prime number [61]. Again, the bases must be chosen independently of each other at random with respect to the uniform distribution on $\{2, 3, \ldots, p - 2\}$. The concrete number of necessary operations depends on the bit length of p, since the numbers for which the worst-case estimates apply decrease significantly in density as the size of the numbers increases.

Optimisations: To optimise the runtime of, for example, Algorithm B.3, it can be helpful to eliminate composite numbers with very small factors by trial division or sieving techniques before applying the probabilistic primality test. Such a preliminary test has only minor impact on the probability that numbers classified as prime by the test are composite. The recommendations on the required number of repetitions of the Miller-Rabin test therefore apply unchanged to variants of the algorithm optimised in this way.

Other Comments: According to [92, Appendix F.2], it is also recommended in this Technical Guideline to perform a verification of the prime number property with 50 rounds of the Miller-Rabin test when generating prime numbers which are to be used in particularly security-critical functions of a cryptosystem or whose generation is not very time-critical. This applies, for example, to prime numbers that are generated once as permanent parameters of a cryptographic mechanism and are then not changed for a long period of time and are possibly used by many users.

A random bit generator of the functionality class PTG.3, DRG.4, DRG.3, or NTG.1 may be used to generate the required random numbers. Until the end of 2022, the use of random number generators of the functionality class PTG.2 is permitted as well. When using a deterministic random number generator, the generation of uniformly distributed prime numbers is from an information-theoretical point of view not possible, but this does not create a security risk: Under cryptographic standard assumptions, a random number generator of the functionality class DRG.3 or DRG.4 generates random numbers with a distribution that cannot be distinguished from an ideal distribution by any known attack with realistic practical effort when using classical computers.

However, it should be noted in this context that the security level of the generated RSA moduli may in this case be limited by the security level of the random bit generation. This would be the case, for example, if a random bit generator with a security level of 100 bits were used to generate RSA keys of a length of 4096 bits.

Alternative Primality Tests: The choice of a primality test is not security critical from a cryptanalytic point of view as long as the selected test does not misclassify prime numbers as composite and as long as the probability that composite numbers pass the test is negligible. Therefore, other tests for which these properties have been demonstrated in the literature may be used in place of the Miller-Rabin test without loss of conformity to this Technical Guideline. However, the use of the very widely known Miller-Rabin algorithm is advantageous with regard to, among other things, a verification of the correctness of an implementation as well as a check of side-channel resistance.

B.5.3. Generation of Prime Number Pairs

To ensure the security of key pairs for which the underlying RSA moduli have been calculated by multiplying two prime numbers generated independently of each other using one of the appropriate methods, it is important that the interval $I := [a, b] \cap \mathbb{N}$ is not too narrow. If key pairs are to be generated whose modulus N has a predetermined bit length n, it is natural to choose $I = [\lceil \frac{2^{(n/2)}}{\sqrt{2}} \rceil, \lfloor 2^{(n/2)} \rfloor] \cap \mathbb{N}$. A different choice of I is compliant with this Technical Guideline if the same interval I is used for p and q and $\mathrm{Card}(I) \geq 2^{-8}b$.

B.5.4. Notes on the Security of the Recommended Methods

In the following, π denotes the prime number function, which is defined as $\pi(x) := \mathrm{Card}(\{n \in \mathbb{N}\colon n \leq x, n \text{ prime}\})$. According to the prime number theorem, $\pi(x)$ is asymptotically equivalent to $x/\ln(x)$, that means,

$$\lim_{x \to \infty} \frac{\pi(x) \cdot \ln(x)}{x} = 1.$$

The security of the methods for prime number generation recommended here is based on the following observations:

the incidence of prime numbers is independent of the chosen residue class

- All three methods can generate any prime number contained in the given interval if the underlying random bit generator can generate all candidates from the respective interval.

- The first two methods generate primes whose distribution is practically indistinguishable from a uniform distribution when the recommended security parameters are used. This is obvious for the first method; for the second method it follows heuristically from *Dirichlet's prime number theorem*: The relative frequency of primes is asymptotically the same in all invertible residue classes modulo S, and the residue class modulo S of the prime to be generated is chosen according to the uniform distribution on $(\mathbb{Z}/S)^*$.

- Strictly speaking, the argument for the security of the second method just given provides no guarantee that for a concrete S and a concrete given interval I the frequency of primes during the search does not in fact depend on the chosen residue class $r \bmod S$. Indeed, it is clear that this asymptotic statement will not be valid when S approaches the order of magnitude of $b - a$. However, it is reasonable to assume that there are no significant differences in terms of prime density between the different residue classes when the number of primes in each residue class is large. The interval I contains $\pi(b) - \pi(a)$ primes, so for each residue class $\bmod S$ $\frac{\pi(b)-\pi(a)}{\varphi(S)}$ primes are expected. For numbers of the order of about 1000 bits, this expected value can be estimated with a small relative error to $\frac{b\ln(a)-a\ln(b)}{\ln(a)\ln(b)\varphi(S)}$ as long as $\varphi(S)$ is small compared to the numerator of the fraction. It is recommended to choose S such that $\frac{b\ln(a)-a\ln(b)}{\ln(a)\ln(b)\varphi(S)} \geq 2^{64}$ holds.

- The qualitative reasoning given above are sufficient to assess the second method as suitable. In the literature, there are more detailed investigations of closely related methods for prime number generation, see for instance [48].

- The third method generates primes that are not uniformly distributed, even though the biases in the distribution of the generated primes are – according to current knowledge – considered to be practically unexploitable by an attacker. The probability of a prime p in the interval I being output by this method is proportional to the length of the prime-free section in the arithmetic sequence $p - kS$, $p - (k-1)S, \ldots, p - S$, p terminated by p. Since the prime density in these arithmetic sequence tends to increase for large S, this effect is expected to be most pronounced for $S = 2$. Again, however, in practice it means only a very limited loss of entropy. One can limit the distribution bias upwards by terminating and restarting the search with a new starting value if no prime has been found after a reasonable number T of steps: In this case, all prime numbers following a gap of length $\geq T$ are output with equal probability.

Appendix C.

Protocols for Special Cryptographic Applications

This chapter deals with protocols that can be used as building blocks of cryptographic solutions. In the current version of this Technical Guideline, this only concerns the Secure Real-Time Transport Protocol (SRTP), as corresponding information for TLS [22], IPsec [23] and SSH [24] has been moved to parts two to four of the Guideline.

In general, the use of established protocols in the development of cryptographic systems has the advantage of being able to fall back on comprehensive public analysis. In contrast, in-house developments can easily contain vulnerabilities that are difficult for a developer to detect. It is therefore recommended that, wherever possible, to prefer generally available, possibly standardised and extensively evaluated protocols to in-house protocol developments.

C.1. SRTP

SRTP is a protocol that supplements the audio and video protocol RTP (Real-Time Transport Protocol) with functions to ensure confidentiality and integrity of the transmitted messages. It is defined in RFC 3711 [7]. SRTP must be combined with a key management protocol as it does not provide its own mechanisms for negotiating a cryptocontext.

Within this Technical Guideline, the following specifications are recommended when using SRTP:

- As a symmetric encryption scheme with combined integrity protection, AES in Galois/Counter Mode as in [79] is recommended.
- As an alternative encryption method, both AES in counter mode and in f8 mode as in [7] are recommended. A SHA1-based HMAC may be used here as integrity protection, since the use of hash functions of the SHA2 or SHA3 family is not specified in [7]. This HMAC may be reduced to 80 bits in the context of the protocol.
- MIKEY [4] should be used as the key management system. The following key management procedures from [4] are recommended: DH key exchange with authentication via PKI, RSA with PKI, and pre-shared keys. In general, only cryptographic mechanisms recommended in this Technical Guideline should be used within MIKEY and SRTP as components.
- zRTP should only be used if it would involve disproportionate high effort to solve the problem of key distribution by a public key mechanism using a PKI or by pre-distributing secret keys.
- It is strongly recommended to use the mechanisms provided in [7] for replay and integrity protection in SRTP. The „sliding window approach“ from [7] should be used. For integrity protection, mechanisms from Chapter 5 should be used.

In applications for the secure transmission of audio and video data in real time, particular attention should be paid to minimise the creation of side channels, for example through data

transmission rate, the chronological order of different signals or other traffic analysis. Otherwise, attacks such as those presented in [6] are possible.

Bibliography

[1] M. Abdalla, M. Bellare, and P. Rogaway. DHIES: An encryption scheme based on the Diffie-Hellman problem. 2001. https://cseweb.ucsd.edu/~mihir/papers/dhies.pdf.

[2] M. R. Albrecht, , D. J. B. T. Chou, C. Cid, J. Gilcher, T. Lange, V. Maram, I. von Maurich, R. Misoczki, R. Niederhagen, K. G. Paterson, E. Persichetti, C. Peters, P. Schwabe, N. Sendrier, J. Szefer, C. J. Tjhai, M. Tomlinson, and W. Wang. Classic McEliece: conservative code-based cryptography. Einreichung zur dritten Runde des NIST PQC Projekts, 2020. https://classic.mceliece.org/nist/mceliece-20201010.pdf.

[3] E. Alkim, J. W. Bos, L. Ducas, P. Longa, I. Mironov, M. Naehrig, V. Nikolaenko, C. Peikert, A. Ragunathan, and D. Stebila. FrodoKEM: Learning With Errors Key Encapsulation. Einreichung zur dritten Runde des NIST PQC Projekts, 2020. https://frodokem.org/files/FrodoKEM-specification-20200930.pdf.

[4] J. Arkko, E. Carrara, F. Lindholm, M. Naslund, and K. Norrman. MIKEY: Multimedia Internet KEYing. RFC 3830, 2004. https://datatracker.ietf.org/doc/html/rfc3830.

[5] atsec information security GmbH. Documentation and Analysis of the Linux Random Number Generator. Dauerstudie im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik, 2021. www.bsi.bund.de/LinuxRNG.

[6] L. Ballard, S. Coull, F. Monrose, G. Masson, and C. Wright. Spot me if you can: recovering spoken phrases in encrypted VoIP conversations. *IEEE Symposium on Security and Privacy*, 2008.

[7] M. Baugher, D. McGrew, M. Naslund, E. Carrara, and K. Norrman. The Secure Real-time Transport Protocol (SRTP). RFC 3711, 2004. https://datatracker.ietf.org/doc/html/rfc3711.

[8] M. Bellare, R. Canetti, and H. Krawczyk. Keying Hash Functions for Message Authentication. In *Advances in Cryptology – CRYPTO 1996*, volume 1109 of *LNCS*, pages 1–15. Springer, 1996.

[9] M. Bellare, R. Canetti, and H. Krawczyk. HMAC: Keyed-Hashing for Message Authentication. RFC 2104, 1997. https://datatracker.ietf.org/doc/html/rfc2104.

[10] M. Bellare and S. K. Miner. A Forward-Secure Digital Signature Scheme. In *Advances in Cryptology – CRYPTO 1999*, volume 1666 of *LNCS*, pages 431–448, 1999.

[11] D. J. Bernstein. Cost analysis of hash collisions: Will quantum computers make SHARCS obsolete? *SHARCS*, 2009.

[12] A. Biryukov, O. Dunkelman, N. Keller, D. Khovratovich, and A. Shamir. Key Recovery Attacks of Practical Complexity on AES Variants With Up to 10 Rounds. In *Advances in Cryptology – EUROCRYPT 2010*, volume 6110 of *LNCS*, pages 299–319, 2010.

[13] A. Biryukov and D. Khovratovich. Related-Key Cryptanalysis of the Full AES-192 and AES-256. In *Advances in Cryptology – ASIACRYPT 2009*, volume 5912 of *LNCS*, pages 1–18, 2009.

[14] S. Blake-Wilson and A. Menezes. Unknown Key-Share Attacks on the Station-to-Station (STS) Protocol. In *Public Key Cryptography*, pages 154–170. Springer, 1999.

[15] D. Bleichenbacher. Chosen ciphertext attacks against protocols based on the RSA encryption standard PKCS# 1. In *Advances in Cryptology – CRYPTO 1998*, volume 1462 of *LNCS*, pages 1–12. Springer, 1998.

[16] H. Böck, J. Somorovsky, and C. Young. Return Of Bleichenbacher's Oracle Threat (ROBOT). In *27th USENIX Security Symposium (USENIX Security 18)*, pages 817–849. USENIX Association, 2018.

[17] A. Bogdanov, D. Khovratovich, and C. Rechberger. Biclique cryptanalysis of the full AES. In *Advances in Cryptology – ASIACRYPT 2011*, LNCS, pages 344–371. Springer, 2011.

[18] D. Boneh and G. Durfee. Cryptanalysis of RSA with private key d less than $N^0.292$. *IEEE transactions on Information Theory*, 46(4):1339–1349, 2000.

[19] D. R. L. Brown. Generic Groups, Collision Resistance, and ECDSA. *Designs, Codes and Cryptography*, 35(1):119–152, 2005.

[20] D. R. L. Brown and R. P. Gallant. The Static Diffie-Hellman Problem. Cryptology ePrint Archive, Report 2004/306, 2004. https://ia.cr/2004/306.

[21] J. Buchmann, E. Dahmen, and A. Hülsing. XMSS - A Practical Forward Secure Signature Scheme Based on Minimal Security Assumptions. In *Post-Quantum Cryptography*, volume 7071 of *LNCS*, pages 117–129. Springer, 2011.

[22] Bundesamt für Sicherheit in der Informationstechnik. BSI TR 02102-2: Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 2 – Verwendung von Transport Layer Security (TLS). www.bsi.bund.de/TR-02102.

[23] Bundesamt für Sicherheit in der Informationstechnik. BSI TR 02102-3: Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 3 – Verwendung von IPsec. www.bsi.bund.de/TR-02102.

[24] Bundesamt für Sicherheit in der Informationstechnik. BSI TR 02102-4: Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 4 – Verwendung von Secure Shell (SSH). www.bsi.bund.de/TR-02102.

[25] Bundesamt für Sicherheit in der Informationstechnik. BSI TR-03116: Kryptographische Vorgaben für Projekte der Bundesregierung. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03116/TR-03116_node.html.

[26] Bundesamt für Sicherheit in der Informationstechnik. BSI TR-03125: Beweiswerterhaltung kryptographisch signierter Dokumente. https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr03125/TR-03125_node.html.

[27] Bundesamt für Sicherheit in der Informationstechnik. Functionality Classes and Evaluation Methodology for Deterministic Random Number Generators. Version 2, 1999. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_20_Functionality_Classes_Evaluation_Methodology_DRNG_e.pdf.

[28] Bundesamt für Sicherheit in der Informationstechnik. A proposal for: Functionality classes and evaluation methodology for true (physical) random number generators. Version 3.1, 2001. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_Functionality_classes_evaluation_methodology_for_true_RNG_e.pdf.

[29] Bundesamt für Sicherheit in der Informationstechnik. A proposal for: Functionality classes for random number generators. Version 2, 2011. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_Functionality_classes_for_random_number_generators_e.pdf.

[30] Bundesamt für Sicherheit in der Informationstechnik. AIS 20: Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren. Version 3, 2013. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_20_pdf.pdf.

[31] Bundesamt für Sicherheit in der Informationstechnik. AIS 31: Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren. Version 3, 2013. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_pdf.pdf.

[32] Bundesamt für Sicherheit in der Informationstechnik. Anhang zu AIS 46: *Minimum Requirements for Evaluating Side-Channel Attack Resistance of RSA, DSA and Diffie-Hellman Key Exchange Implementations*. Version 1, 2013. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_46_BSI_guidelines_SCA_RSA_V1_0_e_pdf.pdf.

[33] Bundesamt für Sicherheit in der Informationstechnik. Anhang zu AIS 46: *Minimum Requirements for Evaluating Side-Channel Attack Resistance of Elliptic Curve Implementations*. Version 2, 2016. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_46_ECCGuide_e_pdf.pdf.

[34] Bundesamt für Sicherheit in der Informationstechnik. BSI TR 3110-2: Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token, Part 2 – Protocols for electronic IDentification, Authentication and trust Services (eIDAS). Version 2.21, 2016. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03110/BSI_TR-03110_Part-2-V2_2.pdf.

[35] Bundesamt für Sicherheit in der Informationstechnik. BSI TR-03111: Elliptic Curve Cryptography. Version 2.10, 2018. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/TechGuidelines/TR03111/BSI-TR-03111_V-2-1_pdf.pdf.

[36] Bundesamt für Sicherheit in der Informationstechnik. Entwicklungsstand Quantencomputer. Version 1.2, 2020. https://www.bsi.bund.de/qcstudie.

[37] Bundesamt für Sicherheit in der Informationstechnik. Migration zur Post-Quanten-Kryptographie. 2020. https://www.bsi.bund.de/PQ-Migration.

[38] Bundesamt für Sicherheit in der Informationstechnik. BSI TR-03116-4: Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 4 – Kommunikationsverfahren in Anwendungen. 2021. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-4.pdf.

[39] Bundesamt für Sicherheit in der Informationstechnik. BSI TR-03116-2: Kryptographische Vorgaben für Projekte der Bundesregierung, Teil 2 – Hoheitliche

Ausweisdokumente. 2022. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03116/BSI-TR-03116-2.pdf.

[40] S. Chen, R. Wang, X. Wang, and K. Zhang. Side-Channel Leaks in Web Applications: A Reality Today, a Challenge Tomorrow. In *2010 IEEE Symposium on Security and Privacy*, pages 191–206. IEEE, 2010. http://research.microsoft.com/pubs/119060/WebAppSideChannel-final.pdf.

[41] J. H. Cheon. Security analysis of the strong Diffie-Hellman problem. In *Advances in Cryptology – EUROCRYPT 2006*, volume 4004 of *LNCS*, pages 1–11. Springer, 2006.

[42] J.-S. Coron, D. Naccache, and J. P. Stern. On the security of RSA padding. In *Advances in Cryptology – CRYPTO 1999*, volume 1666 of *LNCS*, pages 1–18. Springer, 1999.

[43] I. Damgård, P. Landrock, and C. Pomerance. Average Case Error Estimates for the Strong Probable Prime Test. *Mathematics of computation*, 61(203):177–194, 1993.

[44] W. Diffie, P. C. Van Oorschot, and M. J. Wiener. Authentication and Authenticated Key Exchanges. *Designs, Codes and cryptography*, 2(2):107–125, 1992.

[45] ECRYPT – CSA. Algorithms, Key Size and Protocols Report, 2012. https://www.ecrypt.eu.org/ecrypt2/documents/D.SPA.20.pdf.

[46] ECRYPT – CSA. Algorithms, Key Size and Protocols Report, 2018. https://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf.

[47] N. Ferguson. Authentication weaknesses in GCM. *Comments submitted to NIST Modes of Operation Process*, 2005. https://csrc.nist.gov/csrc/media/projects/block-cipher-techniques/documents/bcm/comments/cwc-gcm/ferguson2.pdf.

[48] P.-A. Fouque and M. Tibouchi. Close to uniform prime number generation with fewer random bits. *IEEE Transactions on Information Theory*, 65(2):1307–1317, 2018.

[49] M. Gebhardt, G. Illies, and W. Schindler. A note on the practical value of single hash collisions for special file formats. In *Sicherheit 2006, Sicherheit – Schutz und Zuverlässigkeit*, pages 333–344. Gesellschaft für Informatik e.V., 2006. https://dl.gi.de/bitstream/handle/20.500.12116/24792/GI-Proceedings-77-41.pdf.

[50] D. Gillmor. Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS). RFC 7919, 2016. https://datatracker.ietf.org/doc/html/rfc7919.

[51] L. K. Grover. A fast quantum mechanical algorithm for database search. In *Proceedings of the Twenty-Eighth Annual ACM Symposium on Theory of Computing*, pages 212–219. Association for Computing Machinery, 1996.

[52] N. Heninger, Z. Durumeric, E. Wustrow, and J. A. Halderman. Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices. In *21st USENIX Security Symposium (USENIX Security 12)*, pages 205–220. USENIX Association, 2012. https://www.usenix.org/system/files/conference/usenixsecurity12/sec12-final228.pdf.

[53] R. Housley. Cryptographic Message Syntax (CMS). RFC 5652, 2009. https://datatracker.ietf.org/doc/html/rfc5652.

[54] A. Hülsing, D. Butin, S.-L. Gazdag, J. Rijneveld, and A. Mohaisen. XMSS: eXtended Merkle Signature Scheme. RFC 8391, 2018. https://datatracker.ietf.org/doc/html/rfc8391.

[55] G. Illies, M. Lochter, and O. Stein. Behördliche Vorgaben zu kryptografischen Algorithmen. *Datenschutz und Datensicherheit-DuD*, 35(11):807–811, 2011.

[56] International Organization for Standardization. ISO/IEC 18033-2:2006 Information technology – Security techniques – Encryption algorithms – Part 2: Asymmetric ciphers, 2006.

[57] International Organization for Standardization. ISO/IEC 14888-2:2008 Information technology – Security techniques – Digital signatures with appendix – Part 2: Integer factorization based mechanisms, 2008.

[58] International Organization for Standardization. ISO/IEC 9797-1:2011 Information technology – Security techniques – Message Authentication Codes (MACs) – Part 1: Mechanisms using a block cipher, 2011.

[59] International Organization for Standardization. ISO/IEC 11770-2:2018 Information security – Key management – Part 2: Mechanisms using symmetric techniques, 2018.

[60] International Organization for Standardization. ISO/IEC 14888-3:2018 Information technology – Digital signatures with appendix – Part 3: Discrete logarithm based mechanisms, 2018.

[61] International Organization for Standardization. ISO/IEC 18032:2020 Information security – Prime number generation, 2020.

[62] International Organization for Standardization. ISO/IEC 9796-2:2010 Information technology – Security techniques – Digital signature schemes giving message recovery – Part 2: Integer factorization based mechanisms, 2020.

[63] International Organization for Standardization. ISO/IEC 11770-3:2021 Information security – Key management – Part 3: Mechanisms using asymmetric techniques, 2021.

[64] G. Itkis. Forward Security, Adaptive Cryptography: Time Evolution, 2004. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.95.440.

[65] T. Iwata, K. Ohashi, and K. Minematsu. Breaking and Repairing GCM Security Proofs. In *Advances in Cryptology – CRYPTO 2012*, volume 7417 of *LNCS*, pages 31–49. Springer, 2012.

[66] M. Kaplan, G. Leurent, A. Leverrier, and M. Naya-Plasencia. Breaking symmetric cryptosystems using quantum period finding. In *Advances in Cryptology – CRYPTO 2016*, volume 9815 of *LNCS*, pages 207–237. Springer, 2016.

[67] J. Kelsey, B. Schneier, and D. Wagner. Key-Schedule Cryptanalysis of IDEA, G-DES, GOST, SAFER, and Triple-DES. In *Advances in Cryptology – CRYPTO 1996*, volume 1109 of *LNCS*, pages 237–251. Springer, 1996.

[68] S. Kent. IP Encapsulating Security Payload (ESP). RFC 4303, 2005. https://datatracker.ietf.org/doc/html/rfc4303.

[69] T. Kivinen and M. Kojo. More Modular Exponential (MODP) Diffie-Hellman Groups for Internet Key Exchange (IKE). RFC 3526, 2003. https://datatracker.ietf.org/doc/html/rfc3526.

[70] A. K. Lenstra. Key lengths. contribution to the handbook of information security. 2004. http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.694.8206.

[71] A. K. Lenstra and E. R. Verheul. Selecting Cryptographic Key Sizes. *Journal of cryptology*, 14(4):255–293, 2001.

[72] G. Leurent and T. Peyrin. From Collisions to Chosen-Prefix Collisions Application to Full SHA-1. In *Advances in Cryptology – EUROCRYPT 2019*, volume 11478 of *LNCS*, pages 527–555. Springer, 2019.

[73] G. Leurent and T. Peyrin. SHA-1 is a Shambles: First Chosen-Prefix Collision on SHA-1 and Application to the PGP Web of Trust. In *29th USENIX Security Symposium (USENIX Security 20)*, pages 1839–1856. USENIX Association, 2020. https://www.usenix.org/system/files/sec20-leurent.pdf.

[74] M. Lochter and J. Merkle. Elliptic Curve Cryptography (ECC) Brainpool Standard Curves and Curve Generation. RFC 5639, 2010. https://datatracker.ietf.org/doc/html/rfc5639.

[75] S. Lucks. Attacking Triple Encryption. In *Fast Software Encryption*, volume 1372 of *LNCS*, pages 239–253. Springer, 1998.

[76] S. Lucks and M. Daum. The Story of Alice and her Boss: Hash Functions and the Blind Passenger Attack. Presentation. http://www.cits.rub.de/imperia/md/content/magnus/rumpec05.pdf.

[77] V. G. Martínez, F. H. Álvarez, L. H. Encinas, and C. S. Ávila. A Comparison of the Standardized Versions of ECIES. In *Sixth International Conference on Information Assurance and Security, IAS 2010*, pages 1–4. IEEE, 2010.

[78] D. McGrew, M. Curcio, and S. Fluhrer. Leighton-Micali Hash-Based Signatures. RFC 8554, 2019. https://datatracker.ietf.org/doc/html/rfc8554.

[79] D. McGrew and K. Igoe. AES-GCM Authenticated Encryption in the Secure Real-Time Transport Protocol (SRTP). RFC 7714, 2015. https://datatracker.ietf.org/doc/html/rfc7714.

[80] A. J. Menezes, P. C. V. Oorschot, and S. A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, 1996.

[81] R. C. Merkle. Secure Communications over Insecure Channels. *Communications of the ACM*, 21(4):294–299, 1978.

[82] R. C. Merkle and M. E. Hellman. On the security of multiple encryption. *Communications of the ACM*, 24(7):465–467, 1981.

[83] D. Moody. NIST Status Update on the 3rd Round. Presentation, 2021. https://csrc.nist.gov/Presentations/2021/status-update-on-the-3rd-round.

[84] K. Moriarty, B. Kaliski, J. Jonsson, and A. Rusch. PKCS #1: RSA Cryptography Specifications Version 2.2. RFC 8017, 2016. https://datatracker.ietf.org/doc/html/rfc8017.

[85] National Institute of Standards and Technology. Federal Information Processing Standards NIST FIPS PUB 197: Advanced Encryption Standard (AES), 2001. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf.

[86] National Institute of Standards and Technology. Special Publication NIST SP 800-38A: Recommendation for Block Cipher Modes of Operation: Methods and Techniques, 2001. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38a.pdf.

[87] National Institute of Standards and Technology. Special Publication NIST SP 800-38B: Recommendation for Block Cipher Modes of Operation: The CMAC Mode for Authentication, 2005. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-38b.pdf.

[88] National Institute of Standards and Technology. Special Publication NIST SP 800-38C: Recommendation for Block Cipher Modes of Operation: The CCM Mode for Authentication and Confidentiality, 2007. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-38c.pdf.

[89] National Institute of Standards and Technology. Special Publication NIST SP 800-38D: Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC, 2007. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-38d.pdf.

[90] National Institute of Standards and Technology. Special Publication NIST SP 800-108: Recommendation for Key Derivation Using Pseudorandom Functions, 2009. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-108.pdf.

[91] National Institute of Standards and Technology. Special Publication NIST SP 800-38E: Recommendation for Block Cipher Modes of Operation: The XTS-AES Mode for Confidentiality on Storage Devices, 2010. https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-38e.pdf.

[92] National Institute of Standards and Technology. Federal Information Processing Standards FIPS PUB 186-4: Digital Signature Standard (DSS), 2013. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf.

[93] National Institute of Standards and Technology. Federal Information Processing Standards FIPS PUB 180-4: Secure Hash Standard, 2015. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.180-4.pdf.

[94] National Institute of Standards and Technology. Federal Information Processing Standards NIST FIPS PUB 202: SHA-3 Standard: Permutation-Based Hash and Extendable-Output Functions, 2015. https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf.

[95] National Institute of Standards and Technology. Special Publication NIST SP 800-67: Recommendation for the Triple Data Encryption Standard (TDEA) Block Cipher, 2017. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-67r2.pdf.

[96] National Institute of Standards and Technology. Special Publication NIST SP 800-56B: Recommendation for Pair-Wise Key Establishment Using Integer Factorization Cryptography, 2019. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Br2.pdf.

[97] National Institute of Standards and Technology. Special Publication NIST SP 800-208: Recommendation for Stateful Hash-Based Signature Schemes, 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-208.pdf.

[98] National Institute of Standards and Technology. Special Publication NIST SP 800-56C: Recommendation for Key-Derivation Methods in Key-Establishment Schemes, 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-56Cr2.pdf.

[99] National Institute of Standards and Technology. Special Publication NIST SP 800-57 Part 1: Recommendation for Key Management: Part 1 – General, 2020. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf.

[100] M. Nemec, M. Sys, P. Svenda, D. Klinec, and V. Matyas. The Return of Coppersmith's Attack: Practical Factorization of Widely Used RSA Moduli. In *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pages 1631–1648. Association for Computing Machinery, 2017.

[101] P. Q. Nguyen and I. E. Shparlinski. The Insecurity of the Elliptic Curve Digital Signature Algorithm with Partially Known Nonces. *Designs, Codes and Cryptography*, 30(2):201–217, 2003.

[102] J.-F. Raymond and A. Stiglic. Security Issues in the Diffie-Hellman Key Agreement Protocol. 2000.

[103] T. Ristenpart and S. Yilek. When Good Randomness Goes Bad: Virtual Machine Reset Vulnerabilities and Hedging Deployed Cryptography. In *Network and Distributed System Security Symposium (NDSS) 2010*, 2010.

[104] A. Shamir. How to Share a Secret. *Communications of the ACM*, 22(11):612–613, 1979.

[105] SOG-IS Crypto Working Group. SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, 2020. https://www.sogis.eu/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.2.pdf.

[106] D. X. Song, D. A. Wagner, and X. Tian. Timing Analysis of Keystrokes and Timing Attacks on SSH. In *10th USENIX Security Symposium (USENIX Security 01)*. USENIX Association, 2001. https://www.usenix.org/legacy/events/sec2001/full_papers/song/song.pdf.

[107] M. Stevens, E. Bursztein, P. Karpman, A. Albertini, and Y. Markov. The First Collision for Full SHA-1. In *Advances in Cryptology – CRYPTO 2017*, volume 10401 of *LNCS*, pages 570–596. Springer, 2017.

[108] P. Svenda, M. Nemec, P. Sekan, R. Kvasnovsky, D. Formanek, D. Komarek, and V. Matyas. The Million-Key Question – Investigating the Origins of RSA Public Keys. In *25th USENIX Security Symposium (USENIX Security 16)*, pages 893–910. USENIX Association, 2016. https://www.usenix.org/system/files/conference/usenixsecurity16/sec16_paper_svenda.pdf.

[109] P. C. van Oorschot and M. J. Wiener. A Known-Plaintext Attack on Two-Key Triple Encryption. In *Advances in Cryptology – EUROCRYPT 1990*, volume 473 of *LNCS*, pages 318–325. Springer, 1991.

[110] S. Vaudenay. Security Flaws Induced by CBC Padding - Applications to SSL, IPSEC, WTLS, ... In *Advances in Cryptology – EUROCRYPT 2002*, volume 2332 of *LNCS*, pages 534 – 545. Springer, 2002.

[111] C. Zalka. Grover's quantum searching algorithm is optimal. *Physical Review A*, 60:2746–2751, 1999.