XI симпозиум
«Современные тенденции в криптографии» CTCrypt 2022

On the Preliminary National Standard "Information technology. Cryptographic data security. Terms and definitions"

Alexander Gorin, Alexander Cheryomushkin, Andrey Zubkov

8 june 2022

План

The development and central concepts

The history:

2006 Словарь криптографических терминов. под ред. Погорелова Б.А., Сачкова В.Н.

2021 МР 26.2.006-2021 Технический комитет по стандартизации “Криптографическая защита информации”. Методические рекомендации “Информационная технология. Криптографическая защита информации. Термины и определения.”

2022 Проект ПНСТ “Информационная технология. Криптографическая защита информации. Термины и определения.”

The development and central concepts

The development of the Preliminary Standard had taken **four years**.

Specialists in the thesaurus creation and mathematical linguistics were also involved in this work.

There were three stages of public discussion on preliminary versions within the framework of the Technical Committee for Standardization TC-26 "Cryptographic protection of information" and consulting with Technical Committees TC-362 and TC-331.

Different organizations made a number of comments (**190 in 2020, 180 in 2021, 340 in 2022**), most comments were taken into account when finalizing the text.

Currently, the preliminary National Standard was approved at the XXVIII meeting of the TC-26 and is being prepared for further consideration by the Federal Agency for Technical Regulation and Metrology.

Some comments

There were some comments:

- Russian terms are not a translation of English ones ...
- It is not structured ...
- There are many synonyms ...
- There are some contradictions and inconsistencies with another documents ...
- There are inaccurate citations of existing standards ...
- It does not cover many important modern concepts ...
- and so on

The purpose

The purpose of the document:

- to harmonize international and Russian standards,
- to construct a core system of terms,
- to fix differenses between Russian and English terminology,
- to solve terminology contradictions between different domains of usage.

Preliminary information

International and national standards for Terms and definitions:

- ГОСТ 1.2–2002 Международная система стандартизации. Термины и определения.
- ГОСТ Р ИСО 704–2010 Терминологическая работа. Принципы и методы.
- Р 50.1.075–2011 Разработка стандартов на термины и определения.

In accordance with the established requirements for the development of a terminological standard, 200 terms were selected that reveal the features of the use of cryptographic methods for typical situations.

Central notion

The central notion in the Preliminary Standard is **Cryptosystem**.

It is understood not as a device or facility, but as a union of mathematical algorithms and protocols realized in this device or facility.

2 криптографическая система; криптосистема:

Структурированная совокупность конкретных способов решения поставленных задач защиты информации на основе применения методов криптографической защиты информации.

2 cryptographic system; cryptosystem:

A structured set of concrete solutions of information protection problems based on cryptographic methods of information protection.

3 криптографическая защита информации:

Защита информации с помощью ее криптографического преобразования. [ГОСТ Р 50922-2006, п. 2.2.3]

3 cryptographic protection of information:

Information protection by means of cryptographic transform.

5 криптографическое преобразование:

Процесс преобразования представляющих информацию данных, предназначенный для обеспечения криптографической стойкости и допускающий математическое описание.

5 cryptographic transformation:

The process of transforming the data presenting the information which provides cryptographic security and may be described mathematically.

7 криптографический синтез; криптосинтез:

Область теоретических и прикладных исследований, имеющих целью создание криптографической системы.

cryptographic synthesis:

The field of theoretical and applied research aimed at creating a cryptographic system.

11 криптографический анализ; криптоанализ:

Область теоретических и прикладных исследований, имеющих конечной целью получение обоснованных оценок криптографической стойкости криптографической системы в целом или отдельного криптографического механизма.

cryptographic system analysis; cryptanalysis:

The field of theoretical and applied research with the ultimate goal of obtaining reasonable estimates of the cryptographic security of the cryptographic system as a whole or a separate cryptographic mechanism.

Cryptographic security

13 (криптографическая) стойкость:

Свойство криптографической системы или отдельного криптографического механизма, характеризующее способность противостоять атакам на криптографическую систему (криптографический механизм).

13 (cryptographic) security:

A property of a cryptographic system or a separate cryptographic mechanism that characterizes the ability to withstand attacks on a cryptographic system (cryptographic mechanism).

Security strength

15 практическая стойкость (для конкретной задачи защиты информации):

Оценка средней вычислительной трудоемкости наилучшего известного алгоритма, реализующего успешную атаку на криптографическую систему [криптографический механизм] для конкретных исходных данных о ее [его] функционировании и конкретной задачи защиты информации.

15 security strength (level of security) [for the information protection task]:

Estimation of the average computational complexity of the best known algorithm implementing a successful attack on a cryptographic system [cryptographic mechanism] for specific initial data on its functioning and the specific task of protecting information.

Provable security

16 теоретическая [доказуемая] стойкость :

Характеристика криптографической системы [отдельного криптографического механизма], определенная в рамках некоторой математической модели, описывающей криптографическую систему [криптографический механизм], позволяющая обосновать ее [его] способность противостоять возможным атакам на нее [него] для конкретных исходных данных о ее [его] функционировании и конкретной задачи защиты информации.

16 provable security [for the information protection task]:

A characteristic of a cryptographic system [a separate cryptographic mechanism], defined within the framework of some mathematical model describing a cryptographic system [cryptographic mechanism], which makes it possible to justify its ability to withstand possible attacks on it for specific initial data on its functioning and the specific task of protecting information.

Cryptographic mechanism

8 криптографический механизм:

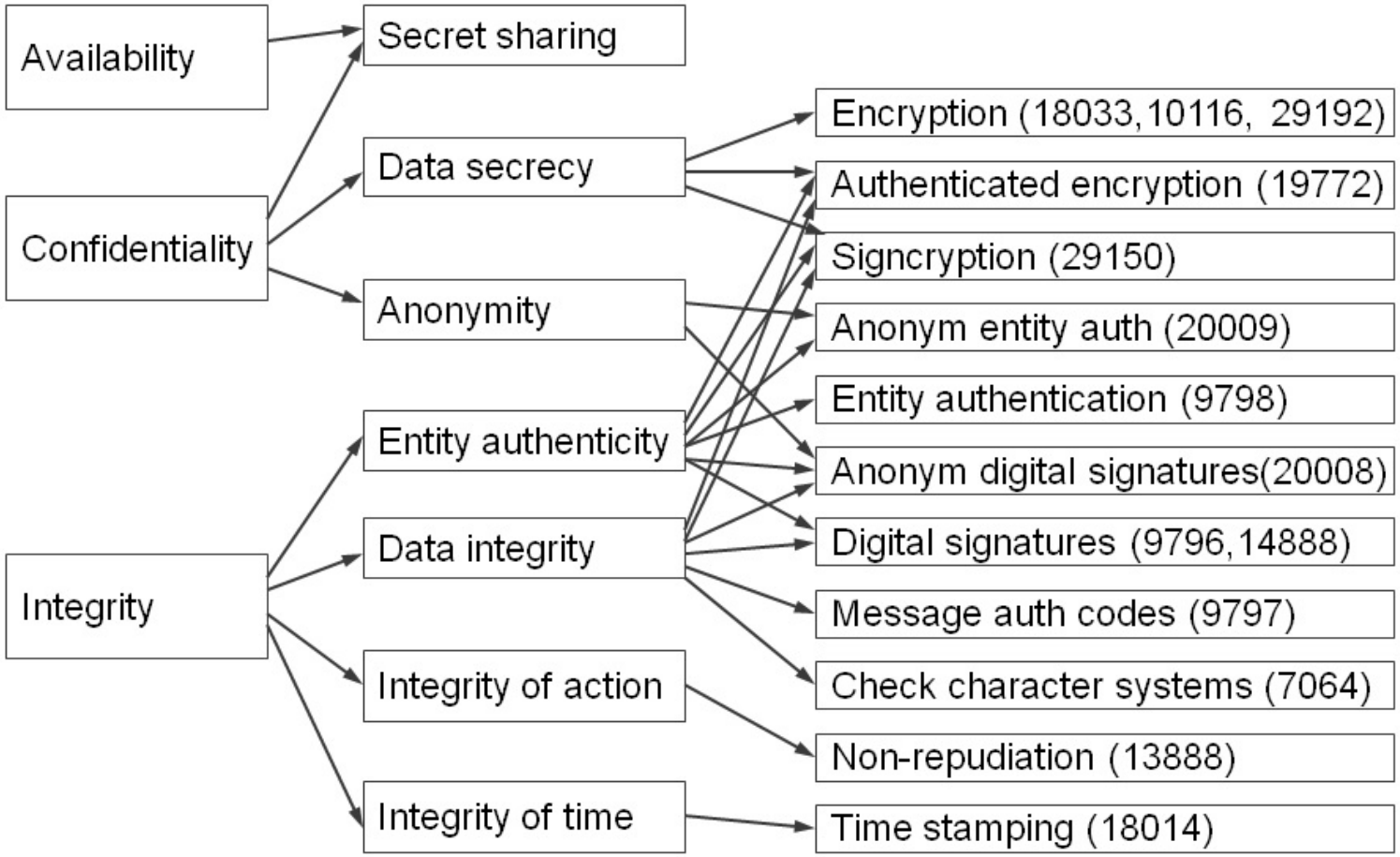
Криптографический алгоритм или криптографический протокол, применяемый в криптографической системе для обеспечения решения конкретной задачи защиты информации или создания и функционирования ее ключевой системы.

3 cryptographic mechanism:

A cryptographic algorithm or cryptographic protocol used in a cryptographic system to provide a solution to a specific task of protecting information or creating and functioning its key system.

WG 2 SD1 – WG 2 Roadmap

Relationships between the objectives and 14 mechanism standards



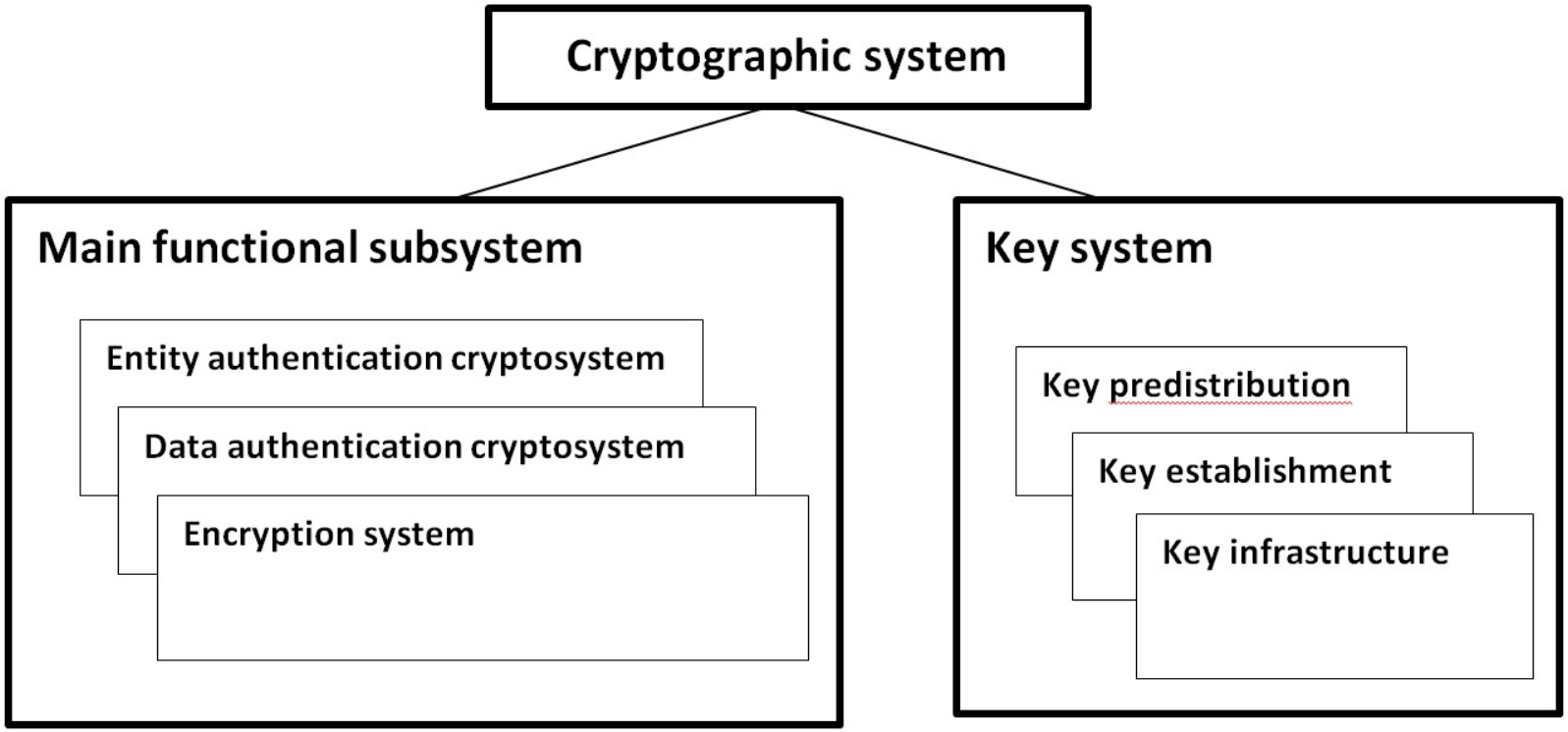
Information protection cryptographic tasks

Cryptographic system may guarantee the following objectives to solve **information protection tasks**:

- **confidentiality** (unauthorized disclosure)
- **entity authenticity** (information interaction)
- **data authenticity**
  - — **data integrity** (modification of information)
  - — **data origin authenticity** (source of information)
- **non-repudiation** (deny the creation or receipt)
- **anonimity** (of the sender and recipient)
  - — untraceability
  - — unlinkability
- time stamping (time substitution)

Types of a cryptosystems

A structure of cryptosystem



Types of a cryptosystems

Types of a cryptosystems:

- (symmetric/asymmetric) **encryption system**
- (symmetric/asymmetric) **entity authentication cryptosystem**
- (symmetric) **data authentication cryptosystem**
- (asymmetric) **digital signature cryptosystem**
- (symmetric/asymmetric) **key system**

Key systems

21 ключевая система:

Подсистема криптографической системы, с помощью которой обеспечивается создание криптографических ключей, необходимых для ее функционирования, и управление ими на основе инфраструктуры управления ключами.

21 key system:

A subsystem of a cryptographic system which ensures the creation of cryptographic keys necessary for its functioning and their control based on the key management system.

Key systems

- symmetric / asymmetric / hybrid
- key generation
- key establishment
  - key transport
  - key agreement
- (centralized) key distribution
- preliminary key distribution
- key management infrastructure
- hierarchy
  - logical key
  - derivation key
- key destruction

38 формирование общего ключа (Нрк. установка общего ключа):

Получение сторонами информационного взаимодействия общего секретного ключа с помощью протокола защищенной передачи ключа, выработанного одной из сторон, протокола совместной выработки общего секретного ключа, либо на основе ключевых материалов, полученных при предварительном распределении секретных ключей.

38 key establishment:

Obtaining by the parties of information interaction of a common secret key using either a secure key transfer protocol developed by one of the parties, or a protocol for the joint computation of a common secret key, or on the basis of key materials obtained during the preliminary distribution of secret keys..

3.23 key establishment: [ISO/IEC 11770-3:2021]

Process of making available a shared secret key to one or more entities, where the process includes key agreement and key transport.

Key transport

39 защищенная передача ключа:

Процесс пересылки криптографического ключа от одной стороны к другой способом, обеспечивающим конфиденциальность, подтверждение и аутентификацию пересылаемого криптографического ключа.

39 key transport:

The process of transferring a cryptographic key from one party to another in a way that ensures confidentiality, confirmation and authentication of the transmitted cryptographic key.

3.25 key transport: [ISO/IEC 11770-3:2021]

Process of transferring a key from one entity to another entity, suitably protected.

40 (совместная) выработка общего секретного ключа:

Формирование двумя или несколькими сторонами общего секретного ключа, реализуемое криптографическим протоколом, при котором стороны обмениваются выработанными случайными данными, причем ни одна из сторон не может уменьшить множество возможных значений формируемого криптографического ключа.

40 key agreement:

The formation of a common secret key by two or more parties, implemented by a cryptographic protocol, in which the parties exchange generated random data, and none of the parties can reduce the set of possible values of the generated cryptographic key.

3.18 key agreement: [ISO/IEC 11770-3:2021]

Process of establishing a shared secret key between entities in such a way that neither of them can predetermine the value of that key.

Key distribution

78 распределение секретных ключей:

Централизованное распределение среди пользователей симметричной криптографической системы секретных ключей, необходимых для ее функционирования.

78 key distribution

Centralized distribution among users of a symmetric cryptographic system of the secret keys necessary for its functioning.

2.21 key distribution [ISO/IEC 11770-1:2010]

Service which securely provides key management information objects to authorized entities.

Preliminary key distribution

81 предварительное распределение секретных ключей:

Централизованное распределение ключевых материалов, с помощью которых пользователи симметричной криптографической системы могут независимо вычислять секретные ключи.

81 preliminary key distribution:

Centralized distribution of key materials with which users of a symmetric cryptographic system can independently calculate secret keys.

Encryption system

26 система шифрования; шифрсистема:

Криптографическая система, выполняющая функцию обеспечения конфиденциальности информации, включающая в себя шифр (код) и ключевую систему.

26 encryption system; enciphering system; ciphersystem:

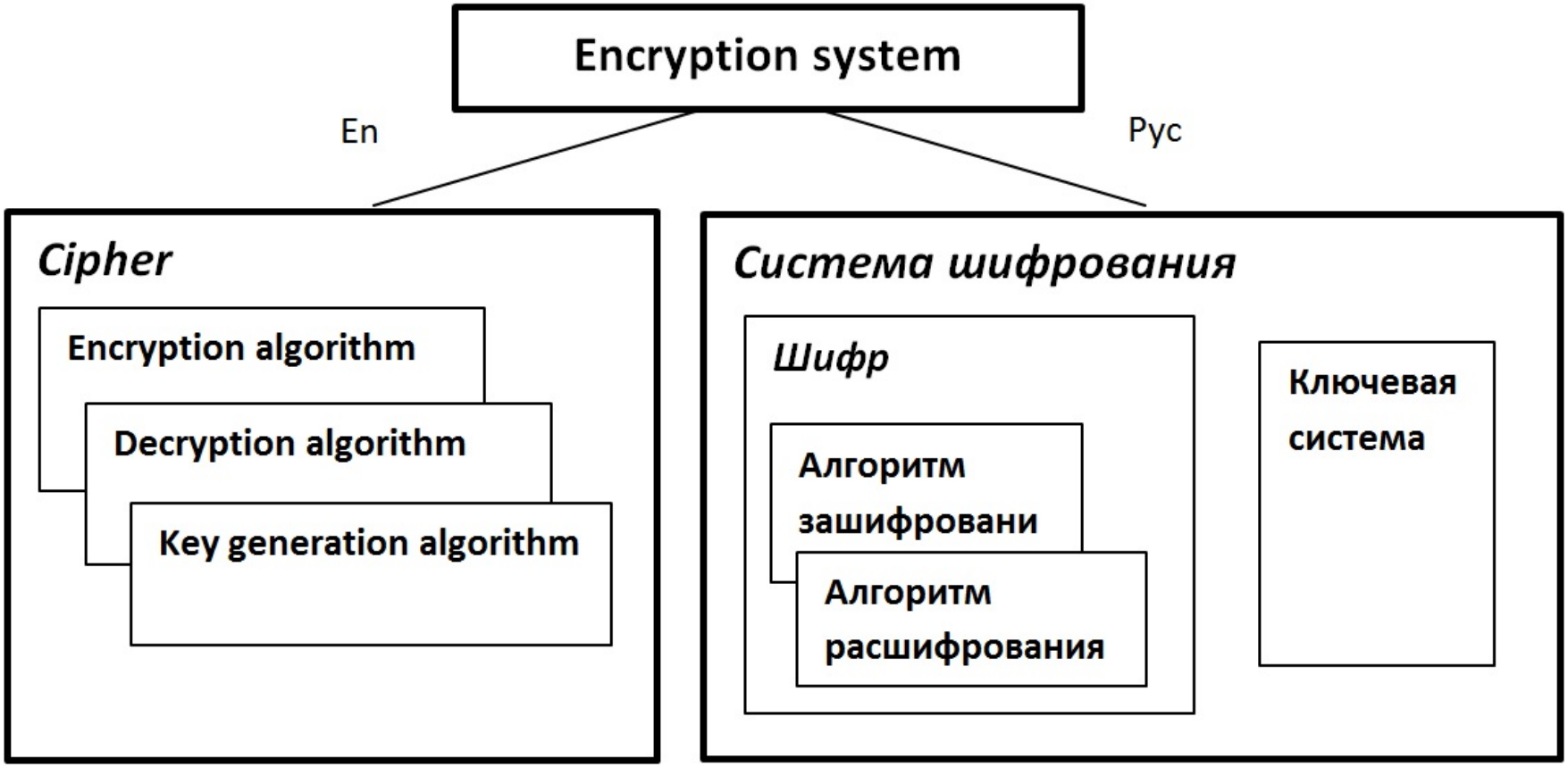
A cryptographic system that performs the function of ensuring the confidentiality of information, including a cipher (code) and a key system.

3.13 encryption system; enciphering system: [ISO/IEC DIS 18033-1:2020]

(reversible) transformation of data by an encryption algorithm to produce ciphertext, i.e. to hide the information content of the data

The encyption system system may be **symmetric/asymmetric/hybrid**.

Encryption system



Cipher

105 шифр:

Семейство определяемых криптографическим ключом и, возможно, вектором инициализации или синхропосылкой, преобразований, определяющих процессы зашифрования и расшифрования, обладающих свойством, что результат применения расшифрования к образу преобразования зашифрования с соответствующим криптографическим ключом, дает первоначальный результат.

105 cipher:

A family of transformations defined by a cryptographic key and, possibly, an initialization vector or a sync message, defining the processes of encryption and decryption, having the property that the result of applying decryption to the image of the encryption transformation with the corresponding cryptographic key gives the initial result.

Types of a encryption systems

Types of ciphers:

- stream cipher
- block cipher
- basic block cipher
- substitution cipher
- code
- permutation cipher

Symmetric encryption system

103 симметричная система шифрования; система шифрования с секретным ключом:

Система шифрования, являющаяся симметричной криптографической системой, в которой для зашифрования и расшифрования применяются одинаковые секретные ключи.

103 symmetric encryption system:

An encryption system that is a symmetric cryptographic system in which the same secret keys are used for encryption and decryption.

3.24 symmetric encryption system: [ISO/IEC DIS 18033-1:2020]

Encryption system based on symmetric cryptographic techniques.

ISO/IEC 29150:2011, 3.41

Asymmetric encryption system

103 асимметричная система шифрования; система шифрования с открытым ключом:

Система шифрования, являющаяся асимметричной криптографической системой, в которой зашифрование осуществляется с использованием открытого ключа получателя, а расшифрование — с помощью личного (закрытого) ключа получателя.

103 asymmetric encryption system:

An encryption system, which is an asymmetric cryptographic system in which encryption is carried out using the recipient's public key, and decryption is carried out using the recipient's private key.

3.2 asymmetric encryption system:

system based on asymmetric cryptographic techniques whose public transformation is used for encryption and whose private transformation is used for decryption. [ISO/IEC 11770-3:2021]

Entity authentication cryptosystem

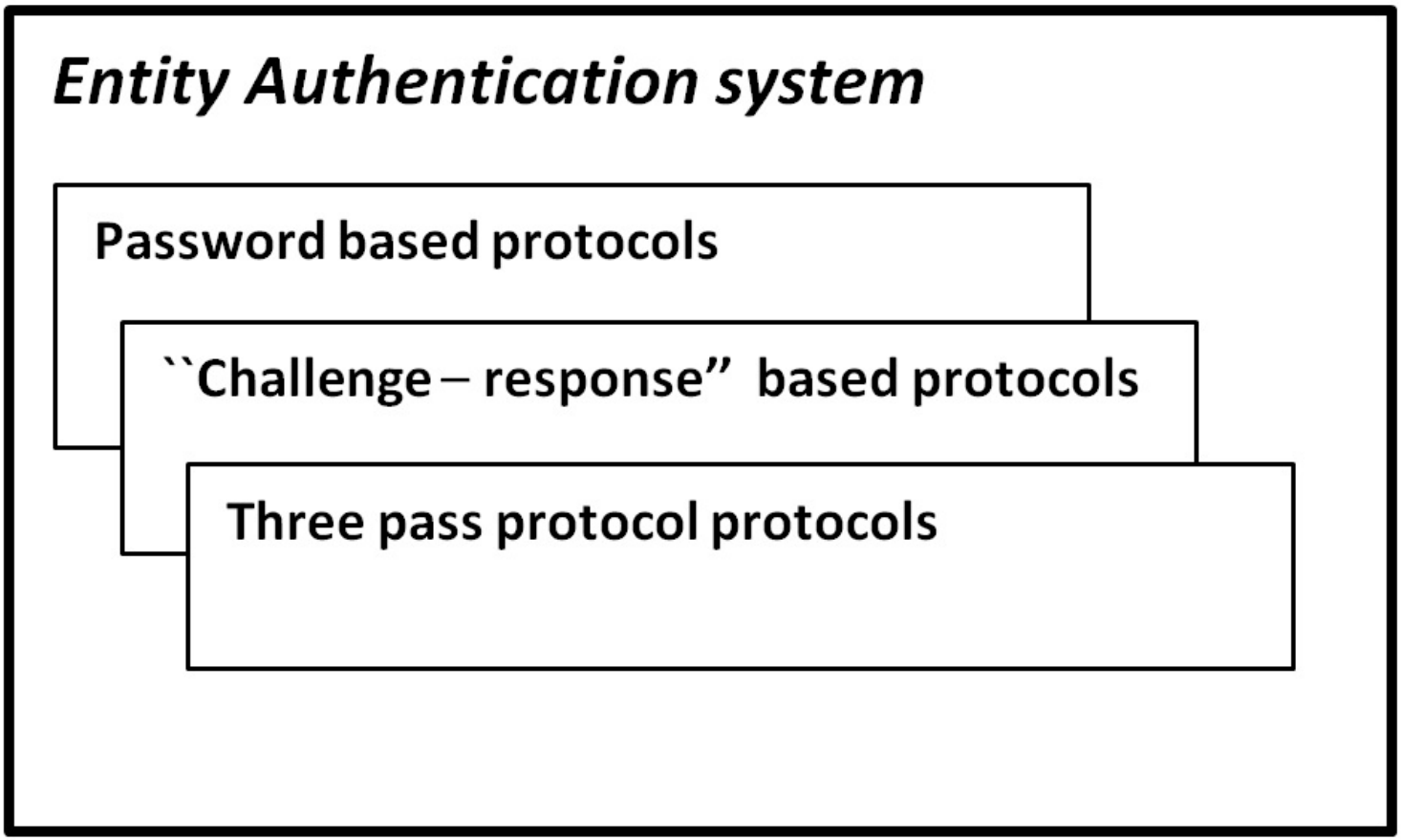
22 криптографическая система аутентификации сторон:

Криптографическая система, включающая в себя криптографический **протокол аутентификации сторон** и **ключевую систему**.

22 entity authentication cryptosystem:

cryptographic system that includes a cryptographic authentication protocol of the parties and a key system.

Entity authentication cryptosystem



Data authentication cryptosystem

23 аутентификация данных:

Проверка целостности данных и аутентификация их источника.

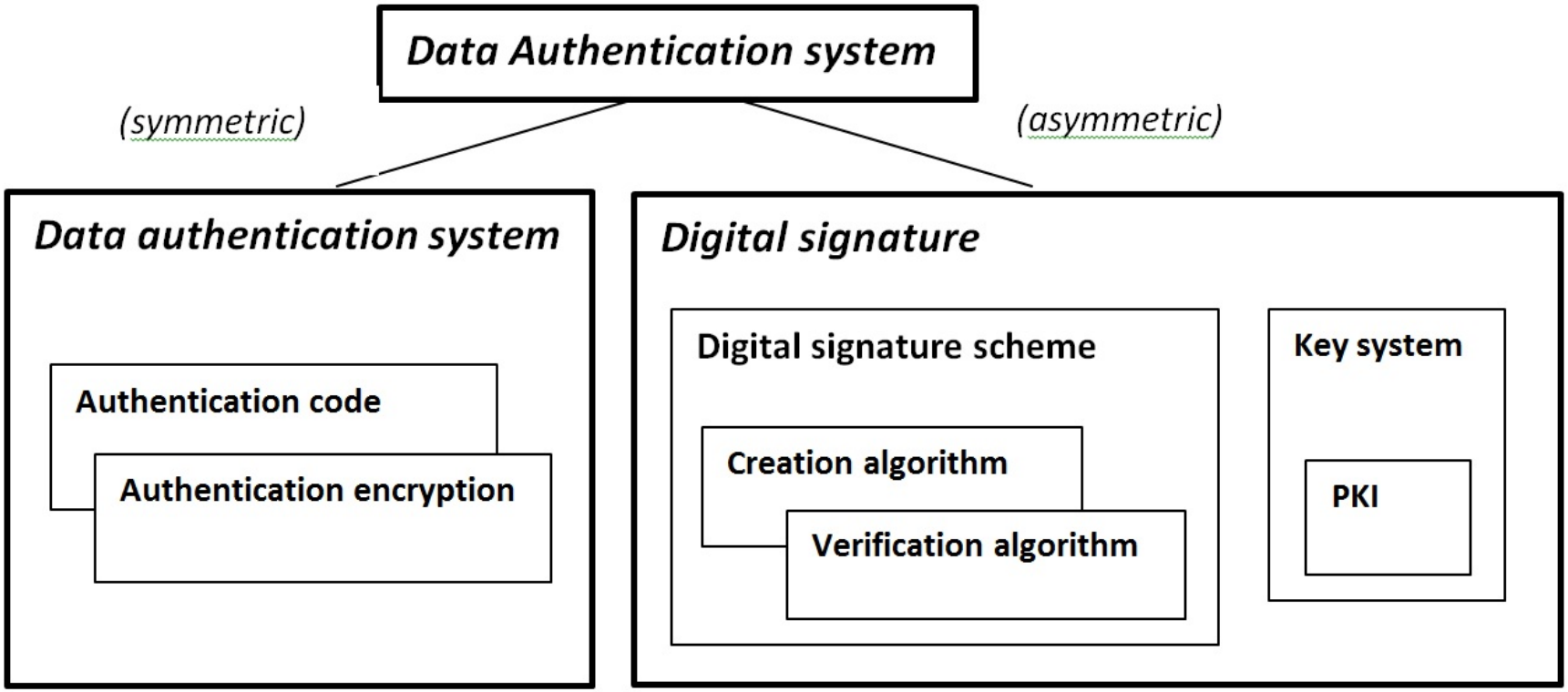
23 data authentication:

Data integrity verification and authentication of their source.

There are two types of **Data authentication cryptosystem**:

- symmetric **data authentication cryptosystem**,
- asymmetric **digital signature cryptosystem**.

Data authentication cryptosystem



Symmetric data authentication cryptosystem

24 система имитозащиты:

Симметричная криптографическая система, выполняющая функцию аутентификации данных, включающая **код аутентификации** и **ключевую систему**.

24 symmetric data authentication cryptosystem:

A symmetric cryptographic system that performs the function of data authentication and includs an authentication code and a key system.

(asymmetric) Digital signature cryptosystem

25 система цифровой подписи:

Асимметричная криптографическая система, выполняющая функцию аутентификации данных, включающая **схему цифровой подписи** и **ключевую систему**.

25 digital signature cryptosystem:

An asymmetric cryptographic system that performs the function of data authentication and includs a **digital signature scheme** and a **key system**.

(asymmetric) Digital signature cryptosystem

134 цифровая подпись:

Результат зависящего от ключа подписи и параметров схемы цифровой подписи криптографического преобразования набора данных (сообщения), обеспечивающий возможность аутентификации источника и проверки целостности набора данных (сообщения) и невозможность отрицания факта создания подписи.

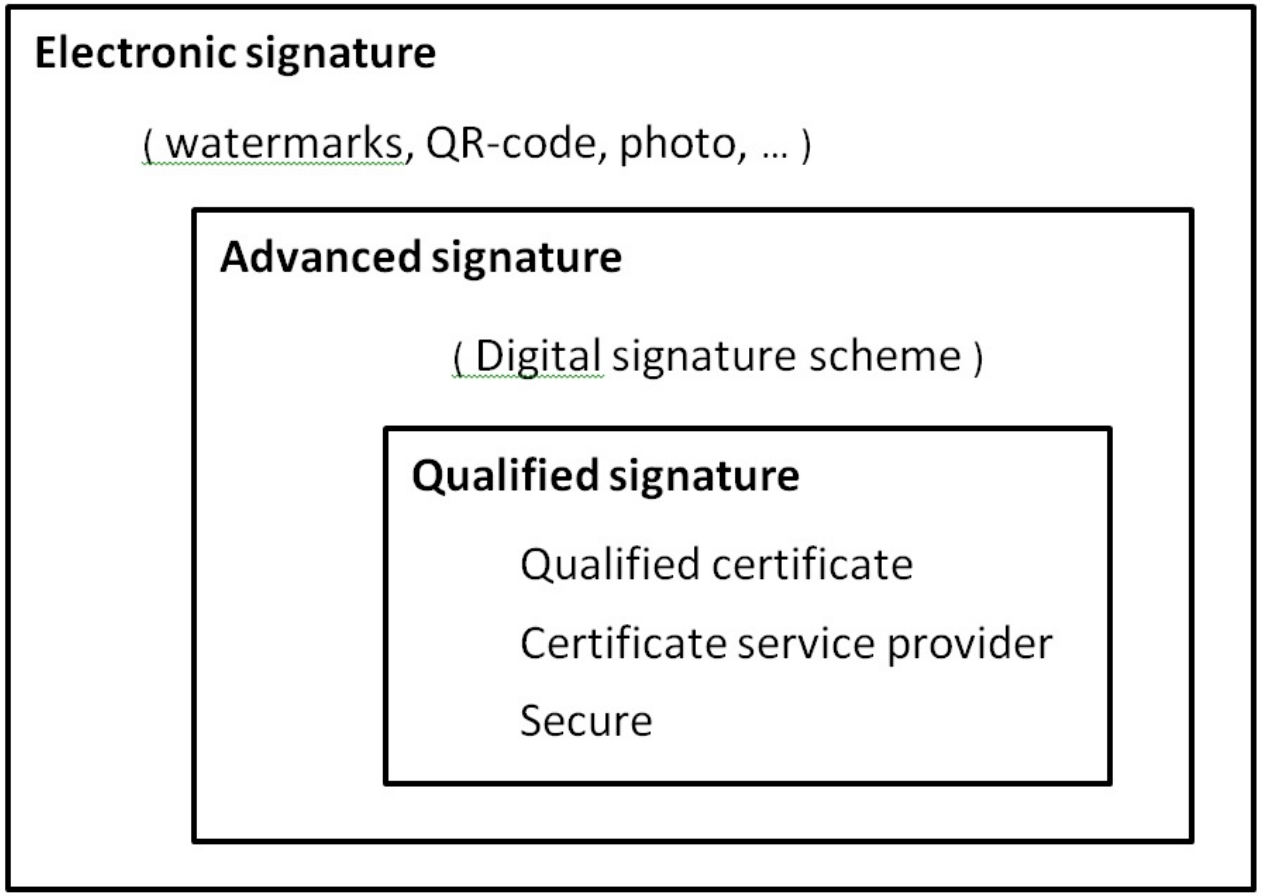
3.3.26 digital signature:

Data appended to, or a cryptographic transformation (see cryptography) of, a data unit that allows a recipient of the data unit to prove the source and integrity of the data unit and protect against forgery e.g. by the recipient. [ISO 7498-2:1989]

Electronic signature

Task	Electronic	Advanced	Qualified
point out the holder	+	+	+
data integrity	−	+	+
data origin authentication	−	+	+
non-repudiation	−	−	+

Types of a electronic signatures



Cryptographic module

К СКЗИ относятся:

- средство шифрования
- средство имитозащиты
- средство электронной подписи
- средство изготовления ключевых документов
- средство кодирования
- ключевой документ

Russian vs English terminology

During last years a number of books, conferences, papers, preprints and so on had appeared in a public domain.

As a rule all such publications are in English.

In many Russian publications on cryptographic topics the authors use individual translations of English terms.

Frequently such translations don't agree with each other or with traditional terminology.

Russian vs English terminology (non-recommended)

As a result, there are many translations for one term, as well as unsuccessful names for well-known concepts.

Russian non-core standards containing definitions of cryptographic terms suffer from the same drawback.

Few Russian standards in the field of cryptographic protection also contain unsuccessful wording of definitions of some terms.

The adopted federal laws introduce even greater confusion, introducing new terms that are not coordinated with either international or Russian standards.

Russian vs English terminology (non-recommended)

Cryptology Cryptography Cryptanalisys	Криптология Криптография Криптоанализ
encipherment/decipherment	зашифрование/дешифрование
cryptographic hash function	криптографическая хеш-функция
message authentication code	код аутентификации
identity-based cryptosystem	личностная криптосистема
lightweit cryptosystem	легковесная криптосистема
substitution attack impersonation attack nonce	подстановка имперсонация нонс

Russian vs English terminology (recommended)

Cryptology Cryptography Cryptanalisys	Криптография Криптографический синтез Криптографический анализ
encipherment/decipherment	зашифрование/расшифрование
cryptographic hash function	не зависящая от ключа к. хеш-функция
MAC algoritm	зависящая от ключа к. хеш-функция
message authentication code	имитовставка
identity-based cryptosystem	к-система на основе идентификаторов
lightweit cryptosystem	низкоресурсная криптосистема
substitution attack impersonation attack nonce	подмена сообщения подмена стороны однократно используемое число

Russian vs English terminology

Non-recommended

session	сессия
padding	паддинг
blind signature	слепая подпись
fixed substitution cipher	шифр фиксированной замены
fresh	свежий

Recommended

session	сеанс
padding	дополнение
blind signature	подпись вслепую
fixed substitution cipher	шифр простой замены
fresh	новое случайное число

Any questions ?