Аутентификация

Аутентификация (authentication)

На основе:

- Знания общего для обоих сторон секрета: слова (пароля) или факта
- Владения уникальным предметом (физическим ключом)
- Обладания уникальными собственными биохарактеристиками

Легальность пользователя может устанавливаться по отношению к различным системам:

- локальный пользователь
- сетевой пользователь
- пользователь почты
- пользователь базы данных
- удаленный пользователь

Децентрализованные системы аутентификации

- многопользовательские приложения
- отдельные операционные системы
- серверы удаленного доступа, маршрутизаторы

Централизованные системы аутентификации

(Принцип единого входа)

- централизованные справочные службы сетевых ОС (NDS, StreetTalk)
- Kerberos
- Tacacs, Radius

Аутентификация

⇒ пользователей

⇒ документов, программных кодов

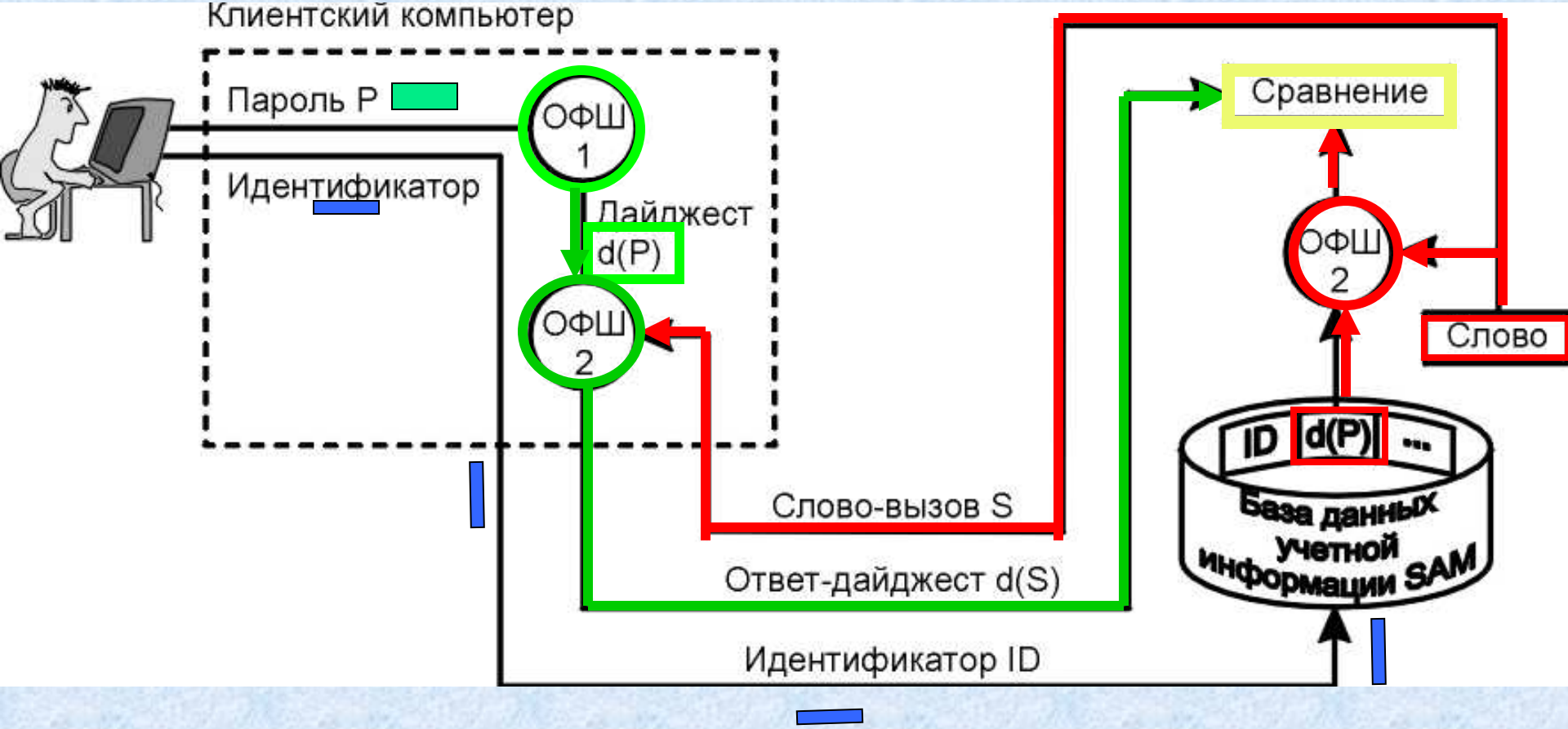
⇒ приложений

⇒ аппаратных средств

Способы аутентификации

- многоразовые пароли
- одноразовые пароли
- слово-вызов (PPP)
- сертификаты
- электронная подпись

Схема сетевой аутентификации на основе многоразового пароля



Используется в Windows NT, протоколе PPP и других системах

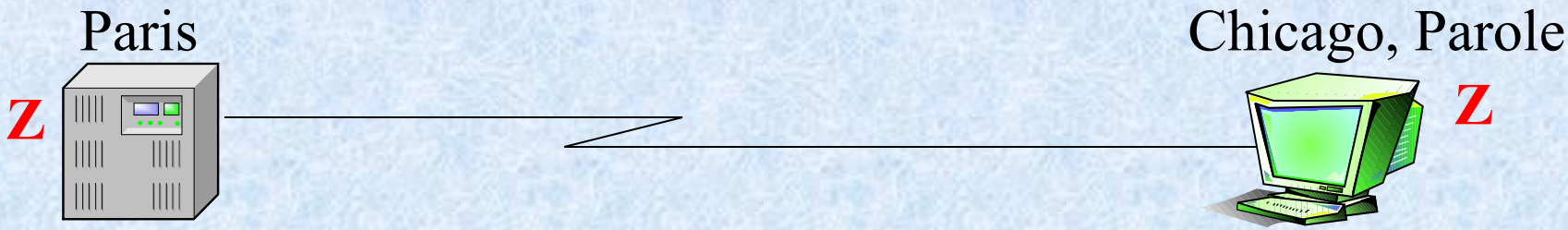
Протоколы аутентификации в протоколе PPP

(RFC 1334)

Password Authentication Protocol (PAP)

Challenge Handshake Authentication Protocol (CHAP)

- Протокол CHAP
  - ⇒ Ключ *(secret)* имеется как у аутентификатора, так и у партнера
  - ⇒ Слово-вызов (*challenge*) генерируется аутентификатором и передается в виде пакета типа Challenge партнеру
  - ⇒ Партнер, получив слово-вызов, зашифровывает его с помощью односторонней хэш-функции MD5
  - ⇒ Результат работы хэш-функции возвращается аутентификатору в виде пакета типа Response
  - ⇒ Аутентификатор сравнивает этот ответ с тем значением, которое он получил, локально применив хэш-функцию к слову-вызову
  - ⇒ Если результаты совпадают, то аутентификация считается успешной и партнеру посылается пакет типа Success - успех
  - ⇒ Для защиты от перехвата ответа аутентификатор должен использовать различные значения последовательности символов при каждой последовательной аутентификации



Установление соединения, ввод имени Chicago 1

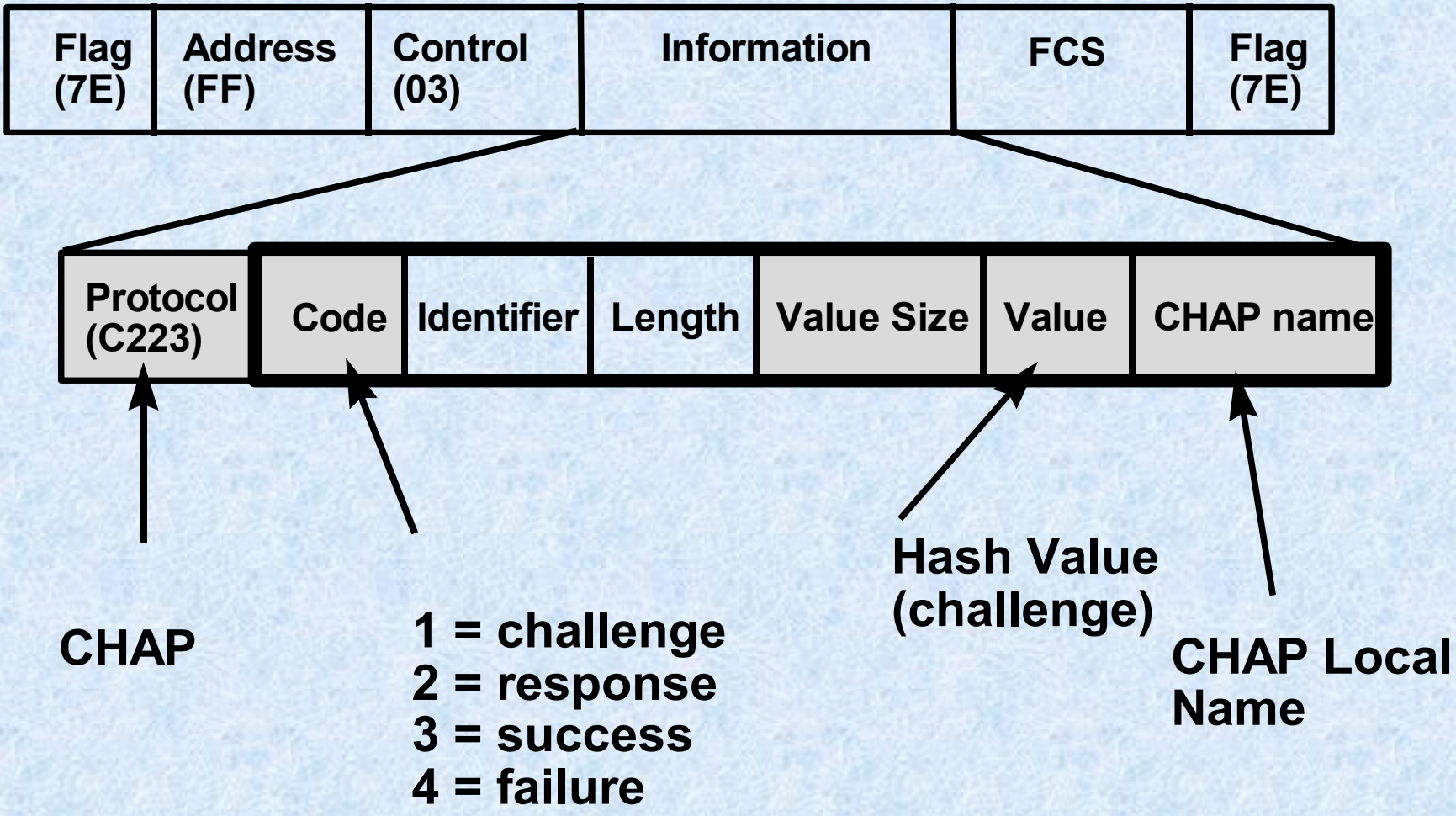
2 Запрос (ID, слово-вызов, Paris)

Ввод пароля, вычисление дайджеста от пароля Z=d(parol),

Отсылка ответа (d(ID, слово-вызов, **Z**), Chicago) 3

3 Извлечение из базы данных дайджеста от пароля Z,
вычисление d(ID, слово-вызов, **Z**),
сравнение с полученным d(ID, слово-вызов, **Z**),
отправка сообщения об успешной аутентификации

Формат пакетов протокола CHAP



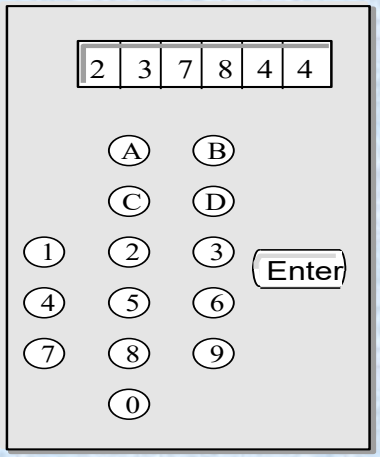
Пример аутентификации узла с именем chicago у аутентификатора с именем paris:

```
- - - - - - - - - - - - - - - - Frame 24 (Challenge)- -- - - - - - - - - - -
ADDR  HEX                ID |длина|длина|слово-вызов |
0000  FF 03 C2 23 01 02 00 0E  04 10 6C 02 F7 70 61 72   □.B#.....l.wpar
0010  69 73                                                          is

- - - - - - - - - - - - - - - - Frame 25 (Response) - - - - - - - - - - - -

PPP:

ADDR  HEX                ID| длина| длина| MD5
0000  FF 03 C2 23 02 02 00 1C  10 47 A4 0C 5D 45 4D EF   □.B#.....G$.]EMo
0010  5D 29 66 B2 13 17 1A F6  4B 63 68 69 63 61 67 6F
])f2...vKchicago
- - - - - - - - - - - - - - - - Frame 26 (Success) - - - - - - - - - - - - -

PPP:

ADDR  HEX                                        ASCII
0000  FF 03 C2 23 03 02 00 04                        □.B#...
```

Одноразовые пароли, основанные на синхронизации по времени

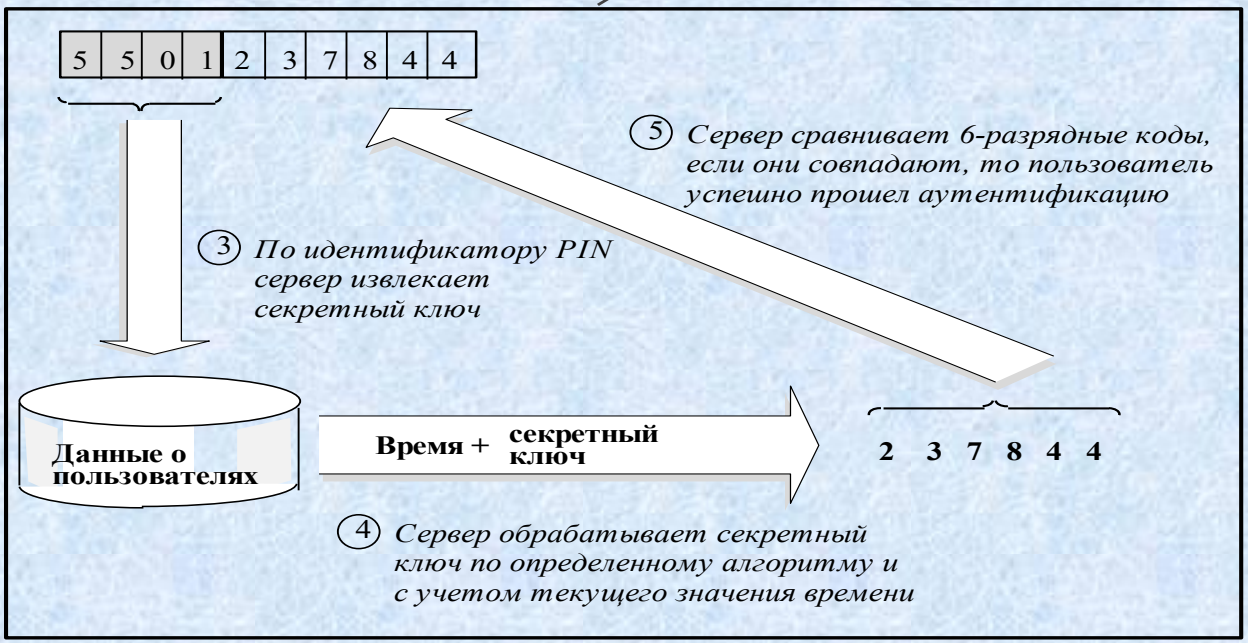
- разработана компанией Security Dynamics
- лицензирована компаниями Cybersafe (Kerberos), IBM (NetSP) и др.
- реализована в коммуникационных серверах компаний Advanced Network and Services, Apple Computer, Cisco Systems, Telebit, Xylogics и Xyplex

① *Токен генерирует 6-разрядный пароль в соответствии с алгоритмом, временем и ключом*

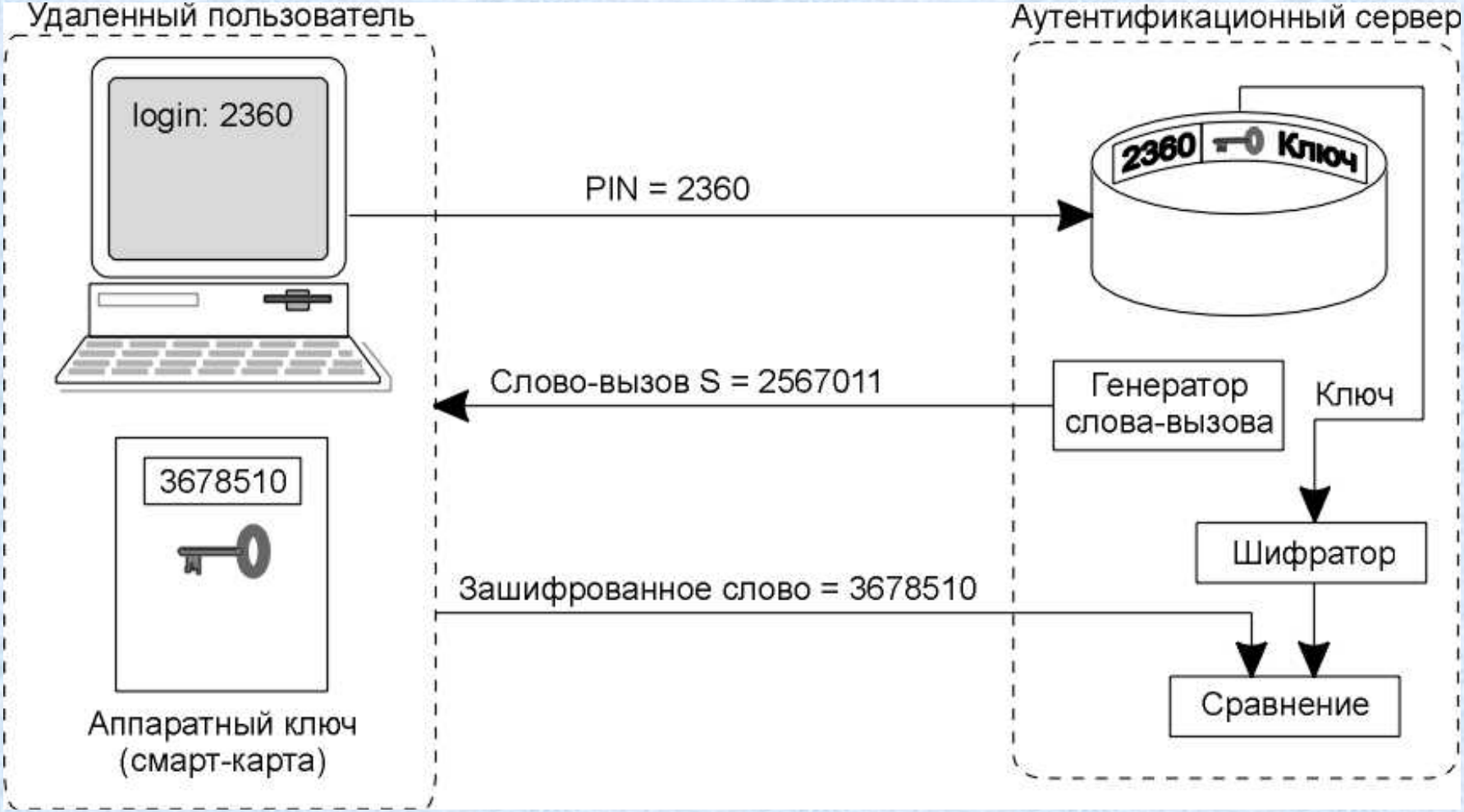


② *При логическом входе пользователь вводит свой идентификатор PIN и 6-разрядный пароль*

Сервер аутентификации



Одноразовый пароль - **слово-вызов**



Программная система аутентификации на основе одноразовых паролей S/Key

1. Инициализация – задание разделяемого секрета X
2. Аутентификатор вычисляет n-кратный дайджест от X и сохраняет его вместо X.
3. Аутентифицируемая сторона вычисляет (n-1)-кратный дайджест и посылает его аутентификатору
4. Аутентификатор вычисляет дайджест от принятого числа и сравнивает его с сохраненным n-кратным дайджестом
5. При каждой новой аутентификации число n уменьшается на единицу.

Аутентификация на основе сертификатов

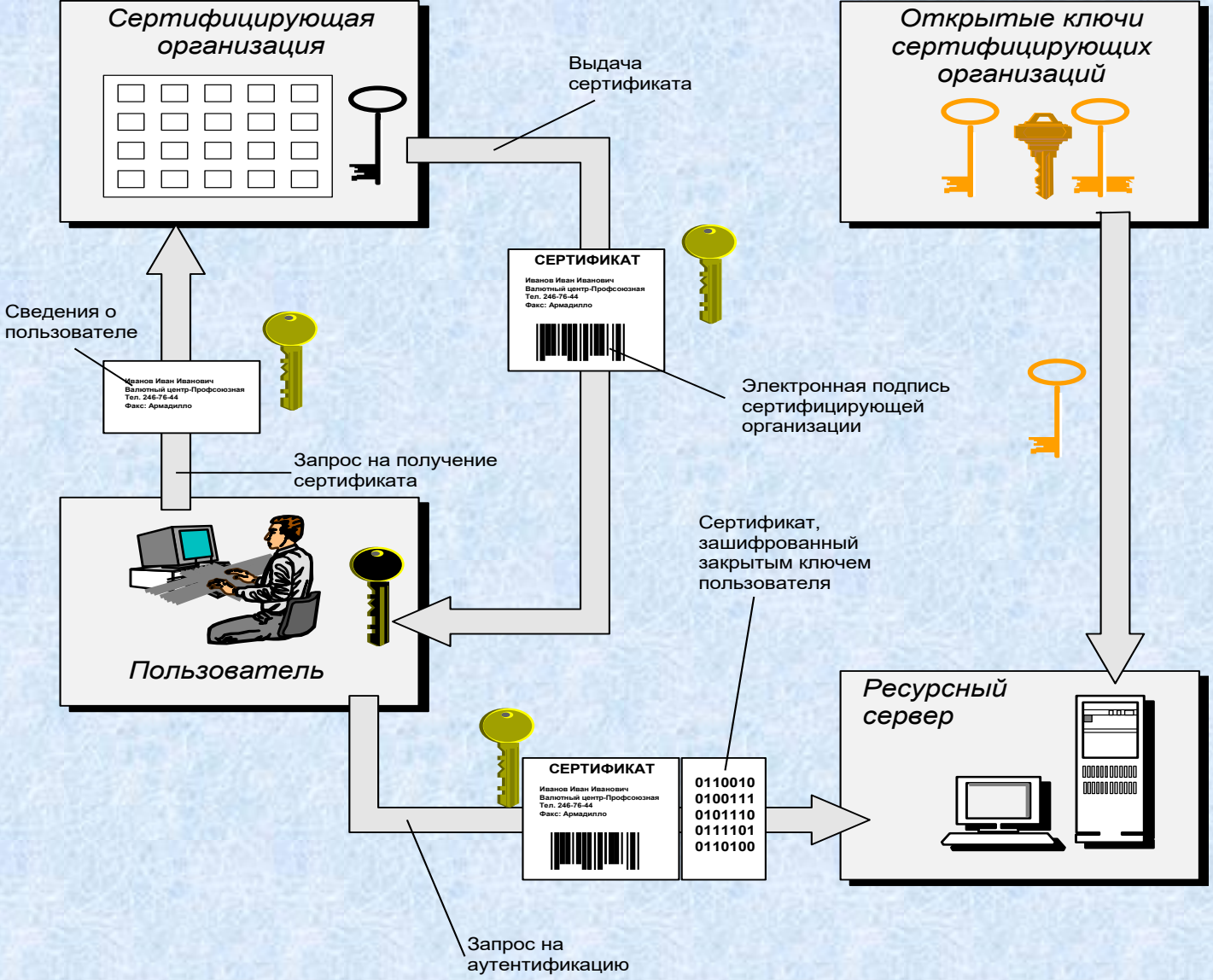
Аутентификация на основе сертификатов

- Масштабируемая схема на основе **открытых ключей**
- **Сертификат (certificate)** – электронный документ:

  (1) гарантирующий соответствие открытого ключа его владельцу

  (2) наделяющий владельца определенными правами по доступу к ресурсам

- Сертификаты выдаются уполномоченными организациями – сертифицирующими центрами (**certificate authority**)


Сертифицирующая организация
Выдача сертификата
Открытые ключи сертифицирующих организаций
СЕРТИФИКАТ
Иванов Иван Иванович
Валютный центр-Профсоюзная
Тел. 246-76-44
Факс: Армадилло
Сведения о пользователе
Иванов Иван Иванович
Валютный центр-Профсоюзная
Тел. 246-76-44
Факс: Армадилло
Электронная подпись сертифицирующей организации
Запрос на получение сертификата
Пользователь
Сертификат, зашифрованный закрытым ключем пользователя
Ресурсный сервер
СЕРТИФИКАТ
Иванов Иван Иванович
Валютный центр-Профсоюзная
Тел. 246-76-44
Факс: Армадилло
0110010
0100111
0101110
0111101
0110100
Запрос на аутентификацию
Открытый и закрытый ключи пользователя
Открытый и закрытый ключи сертифицирующей организации

Сертификат содержит:

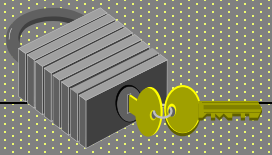
- открытый ключ владельца данного сертификата
- сведения о владельце сертификата, такие, например, как имя, адрес электронной почты, наименование организации, в которой он работает и т.п.
- наименование сертифицирующей организации, выдавшей данный сертификат

Структура сертификата

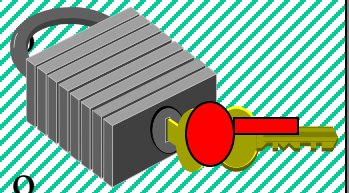
Открытая часть

- Открытый ключ
- Сведения о владельце
- Сведения о сертифицирующем центре

- Открытый ключ
- Сведения о владельце
- Сведения о сертифицирующем центре



- Открытый ключ
- Сведения о владельце
- Сведения о сертифицирующем центре



- Открытый ключ
- Сведения о владельце
- Сведения о сертифицирующем центре

Часть, зашифрованная закрытым ключом СА

Часть, зашифрованная закрытым ключом владельца

Сертифицирующие центры

- Функции: аутентифицируют клиента, «подписывают» информацию о клиенте, фиксируют сертификат в БД
- Клиент-серверная модель
- Выдача сертификата как услуга, например, сертифицирующий центр компании Verisign
- Разные типы сертификатов
- Сертифицирующие центры образуют иерархию

Инфраструктура с открытыми ключами
(Public Key Infrastructure, PKI)

PKI - комплекс программных средств и методик, предназначенных для централизованного администрирования и управления цифровыми сертификатами, парами открытых/закрытых ключей

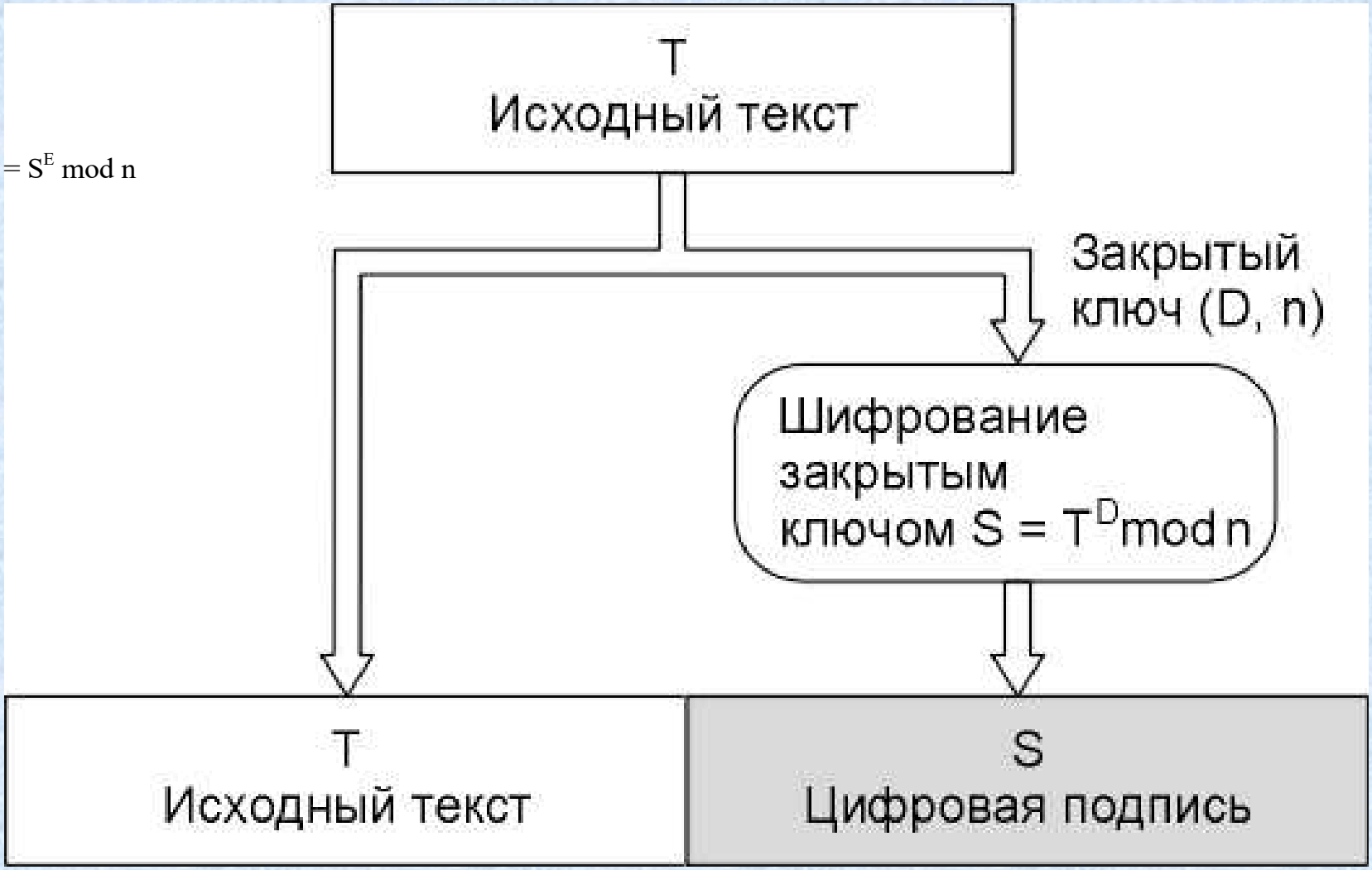
- поддержание базы данных о выпущенных сертификатах
- досрочное прекращение полномочий сертификата
- поддержка списка аннулированных сертификатов
- хранение копий сертификатов, восстановление (*депонирование*) ключей

Цифровая подпись

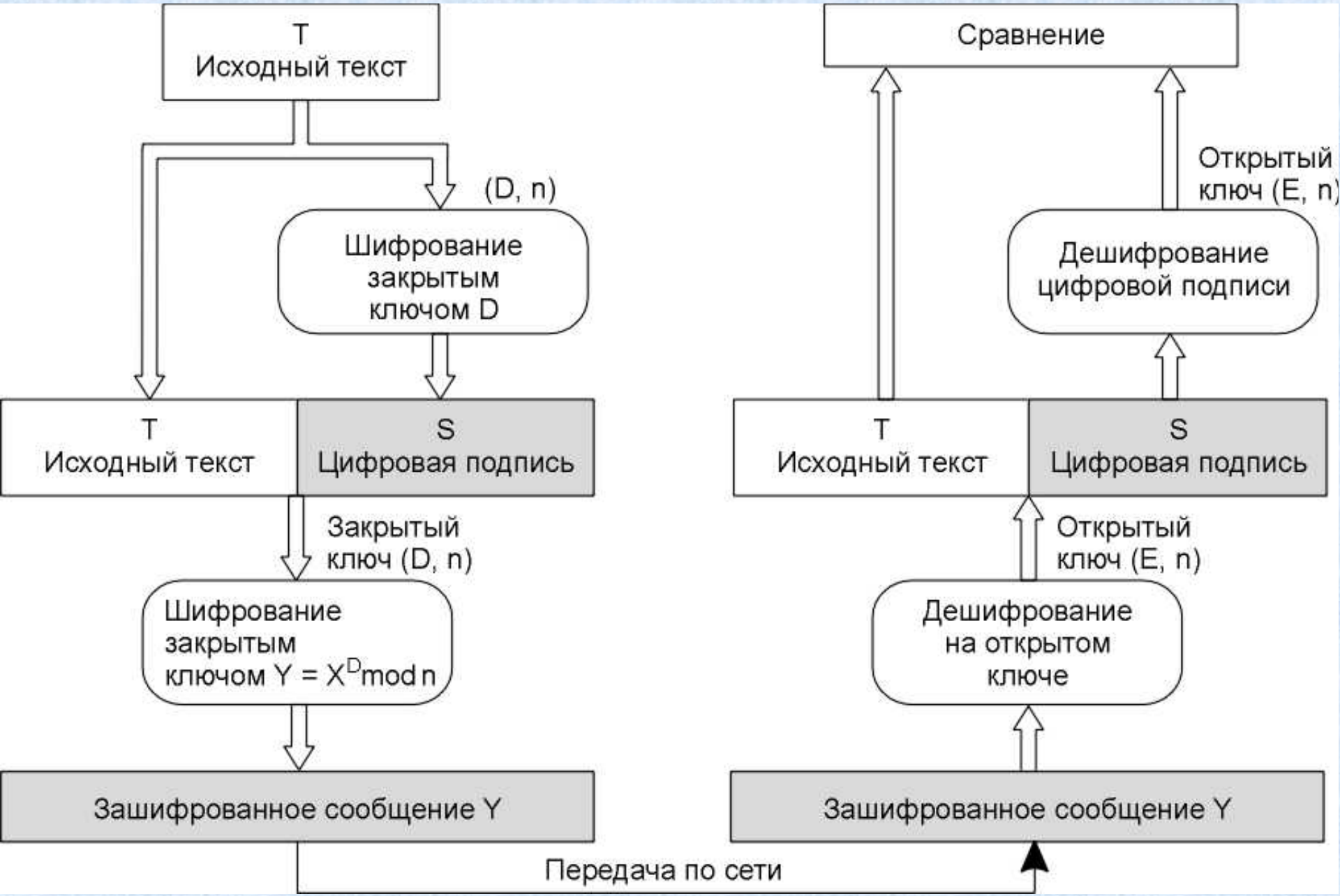
Аутентификация информации - установление подлинности данных, полученных по сети, на основе информации, содержащейся в полученном сообщении

Схема формирования цифровой подписи по алгоритму RSA

$T = S^E \bmod n$



Обеспечение конфиденциальности



Аутентификация программных кодов