Вопросы идентификации и аутентификации в политике безопасности

VI Уральский форум
г. Магнитогорск

Алексей Сабанов, к.т.н.,
Зам. ген. директора ЗАО «Аладдин Р.Д.»

20 февраля 2014г.

Что такое политики безопасности

- Политика безопасности организации (organizational security policies) — совокупность руководящих принципов, правил, процедур и практических приёмов в области безопасности, которые регулируют управление, защиту и распределение ценной информации.

- Согласно ИСО/МЭК 15408-99 «Общие критерии» политика безопасности организации - это одно или несколько правил, процедур, практических приемов или руководящих принципов в области безопасности, которыми руководствуется организация в своей деятельности.

- Политика безопасности устанавливает правила конфигурации систем, действия сотрудников в рабочей обстановке и в случае непредвиденных обстоятельств.

Цели политик безопасности

- обеспечение уровня безопасности, соответствующего нормативным документам предприятия;
- следование экономической целесообразности в выборе защитных мер;
- обеспечение соответствующего уровня безопасности в конкретных функциональных областях банковских ИС;
- обеспечение **подотчетности** всех действий пользователей с информационными ресурсами и анализа регистрационной информации;
- выработка планов восстановления после критических ситуаций и обеспечения непрерывности работы ИС и др.

Идентификация и аутентификация

Идентификация – это сравнение идентификатора, вводимого участником информационного взаимодействия с идентификатором этого участника, зарегистрированном в базе данных;

Аутентификация – это связанные между собой процессы подтверждения **подлинности** предъявленных заявителем идентификаторов (идентификатора) и проверка принадлежности аутентификатора (секрета, который знают обе стороны взаимодействия или о существовании которого знают обе стороны взаимодействия)

Аутентификация и политика ИБ

В Политике ИБ должен быть определен порядок идентификации и аутентификации пользователей для задач:

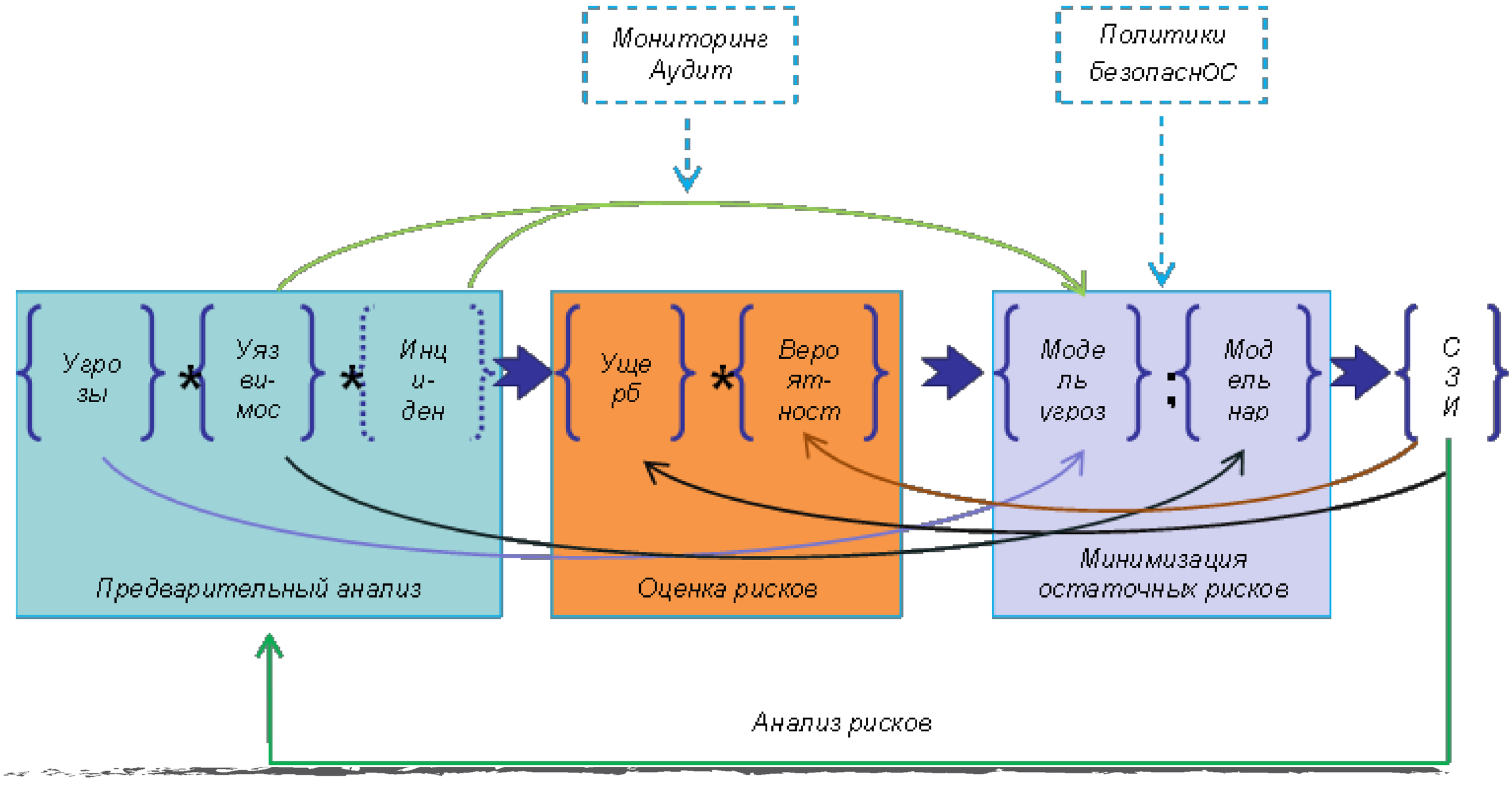
- Доступ пользователей к корпоративной сети и информационным ресурсам банка;
- Удаленный доступ пользователей к внутренним системам;
- Доступ администраторов – требования к аутентификации;
- Доступ к средствам защиты от НСД;
- Доступ клиентов Банка в системах клиент-банк, ДБО, интернет-банкинг;
- Применение электронной подписи.

Классификация механизмов аутентификации

Три вида секрета, три типа аутентификации

Учетная запись пользователя	Секрет (аутентификатор)	Тип аутентификации
логин	**пароль**	**простая**
Логин или поля X.509	**одноразовый пароль (технология OTP) или Закрытый ключ**	**усиленная**
заданные поля X.509, сформированного аккредитованным удостоверяющим центром для доступа пользователя	**закрытый ключ (в терминах №1-ФЗ)**	**строгая**

Общая схема анализа рисков



Угрозы. Верхний уровень

Источник угроз	Вид угрозы	Уровень угрозы
внешний нарушитель	без злого умысла	средний
внешний нарушитель	злонамеренная	высокий
внутренний нарушитель	ошибки	средний
внутренний нарушитель	инсайдер	высокий
техногенные угрозы	аварии	низкий
техногенные угрозы	отказы	средний
техногенные угрозы	сбои	средний
стихийные угрозы	пожары	низкий
стихийные угрозы	наводнения	низкий
стихийные угрозы	землетрясения	низкий
стихийные угрозы	др. форс-мажорные	низкий

ГОСТ Р ИСО/МЭК 13335-1-2006

Процедуры аутентификации

Регистрация нового пользователя ИС.

Хранение идентификационной (ИД) и аутентификационной информации (АИ).

Предъявление ИД и АИ при попытке аутентификации пользователя.

Протоколы аутентификации (подтверждение подлинности АИ).

Процедура валидации (подтверждение принадлежности АИ данному пользователю).

Процедура принятия решения о прохождении аутентификации пользователем.

В случае успешной аутентификации пользователь авторизуется в ИС.

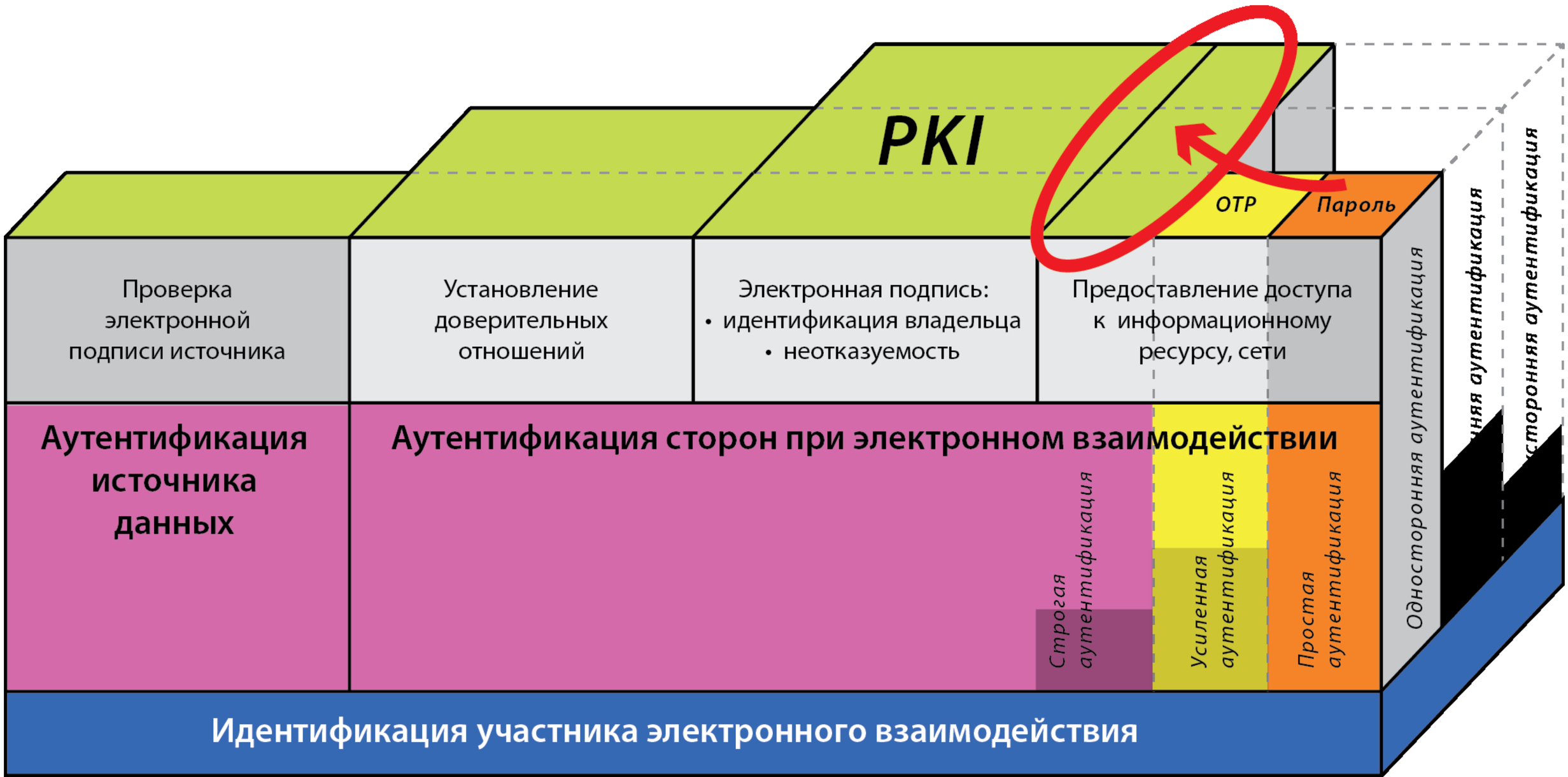
Предъявление аутентификатора

Вид аутентификатора	**Уровень уязвимости**	**Уязвимость предъявления**	**Уровень угрозы**
Пароль	Высокий	Предъявляется в открытом виде	Высокий
Одноразовый пароль	Высокий	Предъявляется и передается по сети в открытом виде	Средний
Закрытый ключ в применяется в оперативной памяти компьютера	Средний	Закрытый ключ нуждается в средствах защиты, например, средствами ОС	Низкий
Процедура подписи производится внутри специально спроектированного чипа устройства SSCD	Низкий	Неизвлекаемость закрытого ключа гарантирована	Низкий

Выбор механизмов и средств аутентификации

- **персонифицированный** доступ пользователей и администраторов;
- безопасный удаленный доступ;
- снижение уровня ошибок администрирования;
- снижение рисков внутренних нарушений;
- обеспечение доказательной базы при нарушениях и конфликтных ситуаций при применении ЭП.

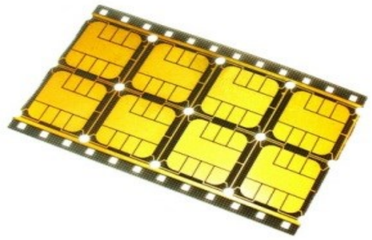
Рекомендуем механизмы аутентификации



Рекомендованные типы аутентификации

	Виды ЭП		
Типы аутентификации	**простая**	**усиленная**	**строгая**
простая	**+**	**-**	**-**
усиленная	**+**	**+**	**-**
строгая	**+**	**+**	**+**

Рекомендуемые технологии и типы ключевых носителей



- **Смарт-карт модули для производства смарт-карт**
  - С RFID
  - С платёжными функциями (эмитируются банками)
  - Дисплейных (OTP)
- **Смарт-карты**
  - Базовый дизайн – VIP: чёрный, палладиевые контакты, серебристое эмбоссирование
  - Опции: встроенный RFID (EM-Marine, HID и др., до 2х меток), расширенная защищённая память до **144** Кб, печать, эмбоссирование
- **PKI- токен для банков**
  - Надёжный и удобный разъем, закрывается колпачком
  - Строгий чёрный дизайн с цветной вставкой
  - Допускает имплантацию **до двух RFID**
  - Разрешён для эксплуатации в ЕС (сертификаты)

Для мобильного доступа - **MicroSD**

Предназначена для мобильных устройств (M2M);

Содержит **чип смарт-карты** (ЭП с неизвлекаемыми закрытым ключом по ГОСТ) и **Flash-память** (4, 8* ГБ);

Может использоваться с переходниками USB, SD (для ПК и ноутбуков), в модемах (“Офис в кармане”).

Спасибо за внимание!