

Аутентификация в формулировках системы ГОСТ Р

Алексей Сабанов, д.т.н.,
Эксперт ISO/JTC1/SC27/WG5
Член ТК 362, ТК 122, ТК 26
доцент МГТУ им. Баумана
Зам. ген. директора ЗАО "Аладдин Р.Д."



Основные виды и методы аутентификации

Целью **идентификации** при доступе субъекта к объекту доступа является распознавание субъекта доступа с необходимой уверенностью в том, что **он является именно тем, за кого себя выдает**.

Целью **аутентификации** является формирование необходимой уверенности в том, что субъект доступа действительно является тем **зарегистрированным** субъектом доступа, за кого себя выдает.

Аутентификация - действия по проверке **подлинности** зарегистрированного субъекта доступа, а также по проверке **принадлежности** субъекту доступа предъявленного идентификатора и аутентификационной информации.

Идентификатор - признак субъекта доступа или объекта доступа в виде строки знаков (символов), который используется при идентификации и однозначно определяет (указывает) соотнесенную с ними идентификационную информацию.

Виды аутентификации

- простая;
- усиленная;
- строгая.

Метод аутентификации - реализуемое при аутентификации predetermined сочетание факторов аутентификации, организации обмена и обработки аутентификационной информации, а также соответствующего данному сочетанию протокола аутентификации.

Правила применения факторов аутентификации

Фактор аутентификации - вид (форма) существования аутентификационной информации, предъявляемой субъектом доступа или объектом доступа при аутентификации.

Факторы аутентификации

- знания: субъект доступа должен знать определенную информацию;
- владения: субъект доступа должен обладать определенным предметом, содержащим аутентификационную информацию;
- биометрический фактор: субъекту доступа должен быть свойственен определенный признак (характеристика), информация (данные) о котором (которой) используется при аутентификации.

При доступе к объекту доступа для аутентификации субъекта доступа необходимо использовать один фактор (однофакторная аутентификация) или несколько факторов (многофакторная аутентификация). При многофакторной аутентификации должны **совместно** применяться не менее двух различных факторов. Доступ к объекту доступа при многофакторной аутентификации должен предоставляться после успешной вторичной идентификации субъекта доступа и положительного результата проверки аутентификационной информации, соответствующей **всем совместно используемым факторам аутентификации**, без доведения субъекту доступа результатов проверки по каждому фактору аутентификации.

Сочетания факторов аутентификации и уровни доверия аутентификации

Аутентификационная информация	Защита аутентификационной информации	Обмен	Факторы аутентификации	Вид аутентификации	Уровень доверия к результату аутентификации
пароль	защита пароля от известных атак	односторонний	знание	простая	низкий
одноразовый пароль	доверенный ДСЧ, защита канала распределения ОТР, защита от MitM-атак	односторонний	владение		
одноразовый пароль	защита операций аутентификации в обоих каналах	односторонний	владение		средний
одноразовый пароль	защита устройства	односторонний	владение		
одноразовый пароль + многоразовый пароль	защита многоразового пароля	односторонний	владение + знание	усиленная	высокий
одноразовый пароль + многоразовый пароль	защита устройства и многоразового пароля	односторонний	владение + знание или биометрия		
криптографические ключи	защита ключей	односторонний или взаимный	владение		
криптографические ключи	защита устройства	односторонний или взаимный	владение + знание		
криптографические ключи	защита ключей	взаимный	владение + знание	строгая	очень высокий
криптографические ключи	защита устройства, содержащего ключ	взаимный	владение + знание или биометрия		
криптографические ключи	защита устройства, содержащего ключ	взаимный	владение + знание и/или биометрия		самый высокий

уровень доверия (assurance level): степень доверия, соответствующая специальной шкале, применяемой в методе обеспечения доверия.

Примечания

1 Уровень доверия не измеряется количественными показателями.

2 Степень доверия обычно определяется усилиями, затраченными на выполнение определенных действий.

[ГОСТ Р 54581–2011/ISO/IEC/TR 15443-1:2005, пункт 2.10]

Внешние и внутренние угрозы аутентификации

Источник угроз	Вид угрозы	Уровень угрозы
внешний нарушитель	без злого умысла	низкий
внешний нарушитель	злонамеренная	высокий
внутренний нарушитель	ошибки	средний
внутренний нарушитель	Злонамеренная - 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

Актуальные угрозы от внешнего нарушителя: угадывание паролей, подслушивание, воспроизведение аутентификационного сообщения, перехват, имитация проверяющей стороны, «человек посередине»

Методы парирования некоторых актуальных внешних угроз

Противодействие угадыванию паролей. Протокол аутентификации устойчив по отношению к атакам угадывания пароля, если злоумышленник, не имеющий априорного знания о пароле, не имеет возможности выявления пароля повторяющимися попытками аутентификации с предполагаемыми паролями. На это влияют и энтропия паролей, и сам протокол. Системы парольной аутентификации могут противостоять атакам угадывания путём требования применения только высокоэнтропийных паролей, обязательного применения ограничения количества неудачных попыток аутентификации либо частоты этих попыток. Для противостояния атакам на пароли, не направленных на конкретного пользователя, проверяющая сторона может также использовать средства обеспечения сетевой безопасности.

Противодействие подслушиванию. Злоумышленник, записавший выполнение протокола, устойчивого к прослушиванию, и имеющий возможность анализа этих записей, не сможет получить сведения, которые позволили бы ему узнать закрытый ключ, секретный ключ, пароль или иную информацию, которая позволила бы ему представиться заявителем. В данном случае отсутствие возможности означает, что попытки ведут к весьма маловероятному успеху, что количество криптографических операций, необходимых для успеха, как минимум, должно составлять 2^{80} , что количество возможных попыток пренебрежимо мало по сравнению с количеством возможных ключей или паролей.

Противодействие воспроизведению. Протокол аутентификации противодействует атакам воспроизведения, если невозможно осуществить успешную аутентификацию путём записи и последующего воспроизведения сообщения аутентификации.

Противодействие перехвату. Протоколы аутентификации и передачи сообщений противостоят перехвату, если злоумышленник не может тайно вставлять, удалять или перенаправлять сообщения, а также вносить изменения в любую информацию, пересылаемую между заявителем и доверяющей стороной.

Противодействие имитации проверяющей стороны. Протокол аутентификации противостоит имитации проверяющей стороны, если злоумышленник не может узнать значение аутентификатора, выступая в роли проверяющей стороны.

Противодействие атаке «человек посередине». Протоколы аутентификации противодействуют атакам «человек посередине», если заявитель и проверяющая сторона взаимодействуют таким образом, который обеспечивает невозможность незаметного участия третьей стороны.

Средства аутентификации

Средства аутентификации - технические (аппаратные) или виртуальные устройства, содержащие информацию о его обладателе, которая может использоваться при идентификации и/или аутентификации



Проблемы управления, связанные с аутентификацией

Доступ пользователей

Токены/смарт-карты, защищенные носители,
устройства IoT, etc.

Сертификаты, ключевые контейнеры, СКЗИ, etc.

Удостоверяющие центры (Certificate Authority)

Службы каталогов

Google Authenticator, Яндекс.ключ, Microsoft
Authenticator, etc.



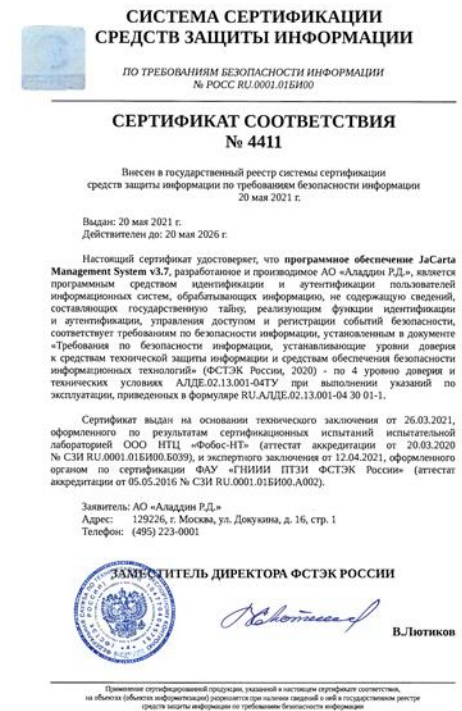
CERTIFICATE
AUTHORITY



JMS 3.7: актуальная версия для платформы Windows

- Закрывает все вопросы в части управления инфраструктурой PKI в перспективе нескольких лет;
- Обеспечивает второй фактор усиленной аутентификации для организаций масштаба предприятия (IAS);
- **Сертифицирована ФСТЭК на соответствие УД-4 по требованиям 76 приказа ФСТЭК России.**

Сертификат ФСТЭК России № 4411 подтверждает, что программное обеспечение JaCarta Management System версии 3.7 является системой управления средствами аутентификации и сертификатами пользователей, а также выполняет функции сервера усиленной аутентификации при использовании данного вида аутентификации в информационных системах, в которых обрабатывается информация, не содержащая сведений, составляющих государственную тайну. JaCarta Management System версии 3.7 соответствует требованиям по безопасности информации по 4 уровню доверия и требованиям технических условий. Сертификат действителен до 20 мая 2026 года.



Функциональные возможности JMS 3.7 (JAS Inside)

Ключевые носители пользователей

Токены/смарт-карты, защищенные носители, устройства IoT,

JaCarta	Рутокен	Gemalto	ESMART	Крипто Про DSS	Реестр
JaCarta (линейка)	Рутокен (линейка)	eToken (линейка)	ESMART (линейка)	Крипто Про DSS	APM
JaCarta-2 (линейка)	Рутокен ЭЦП 2.0				Пользователя
JaCarta-3* (линейка)	Рутокен OTP				
JaCarta WebPass	Рутокен U2F				
JaCarta U2F					

CSP, СКЗИ, etc.

Аладдин	Крипто Про	ИнфоТеКС	Microsoft	Gemalto	Актив
Криптотокен	Крипто Про CSP 3.9	VipNet CSP 4.0	MS Base Smart Card CSP	eToken Base CSP	Active CSP
	Крипто Про CSP 4.0	VipNet CSP 4.2			Рутокен ЭЦП
	Крипто Про CSP 5.0	VipNet CSP 4.4	MS Enhanced CSP		



JaCarta Authentication Server 1.7

Режимы аутентификации

- Только OTP
- OTP + OTP PIN-код
- Доменный пароль Windows + OTP
- Доменный пароль Windows + OTP + PIN-код
- U2F
- SMS

Алгоритмы генерации OTP

- RFC 4226
- TOTP HMAC-SHA-1 (6 цифр)
- TOTP HMAC-SHA-256 (6/7/8 цифр)
- RFC 6238
- TOTP HMAC-SHA1 (6/7/8 цифр)
- TOTP HMAC-SHA256 (6/7/8 цифр)
- TOTP HMAC-SHA512 (6/7/8 цифр)

Поддерживаемые “из коробки” платформы

Palo Alto, Citrix, Check Point, VMWare, Fortinet, Cisco, Microsoft RDG, Microsoft OWA

Крипто Про (NGate) ...

Что даёт использование LiveOffice



• Возможности

- Использование личных компьютеров сотрудников при работе на "удалёнке"
- Удалённое подключение к своему служебному компьютеру и/или к виртуальному рабочему столу
- Удалённая работа в привычной среде, с набором привычных приложений и документов - как в офисе
- Работа с документами ограниченного распространения
- Работа с различными системами электронного документооборота (ЭДО) и использование электронной подписи (ЭП)
- Выход в Интернет - только со служебного компьютера через корпоративный шлюз и корпоративные средства защита

Что даёт использование LiveOffice

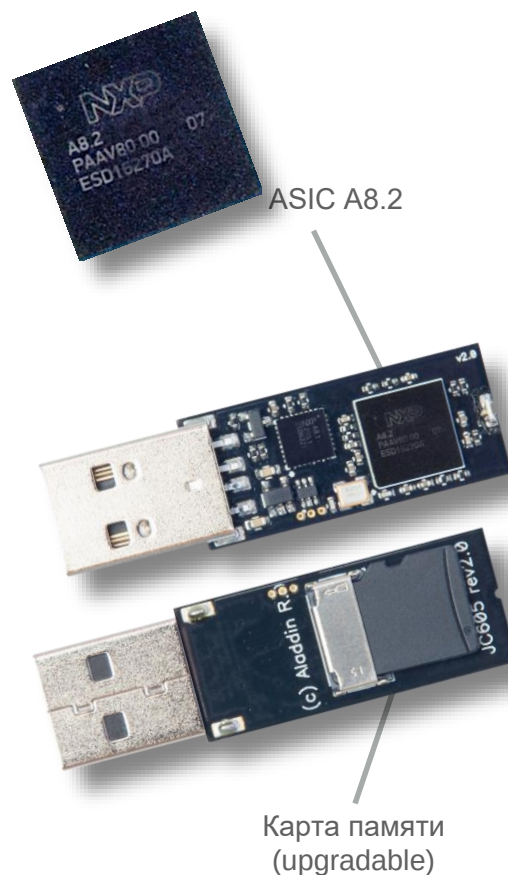


• Решение не позволяет

- Копировать обрабатываемую информацию на локальные, съёмные диски, флеш-накопители и на другие устройства
- Загрузить какой-либо файл (возможно, зараженный) на свой служебный ПК
- Распечатать обрабатываемую информацию на подключенный локальный или сетевой принтер
- Напрямую выходить в Интернет с личного ПК (во время работы LiveOffice)
- Раскрыть обрабатываемую информацию в случае утери или кражи USB-устройства
- Скомпрометировать пароль для удалённого подключения к служебному ПК
 - При развёрнутой PKI для 2ФА пользователя используются цифровые сертификаты
 - Если PKI не развёрнута, то используется технология SecurLogon - подстановка сложного длинного пароля, который неизвестен пользователю (а следовательно, он не сможет использовать его при заказе пиццы или в соцсетях)



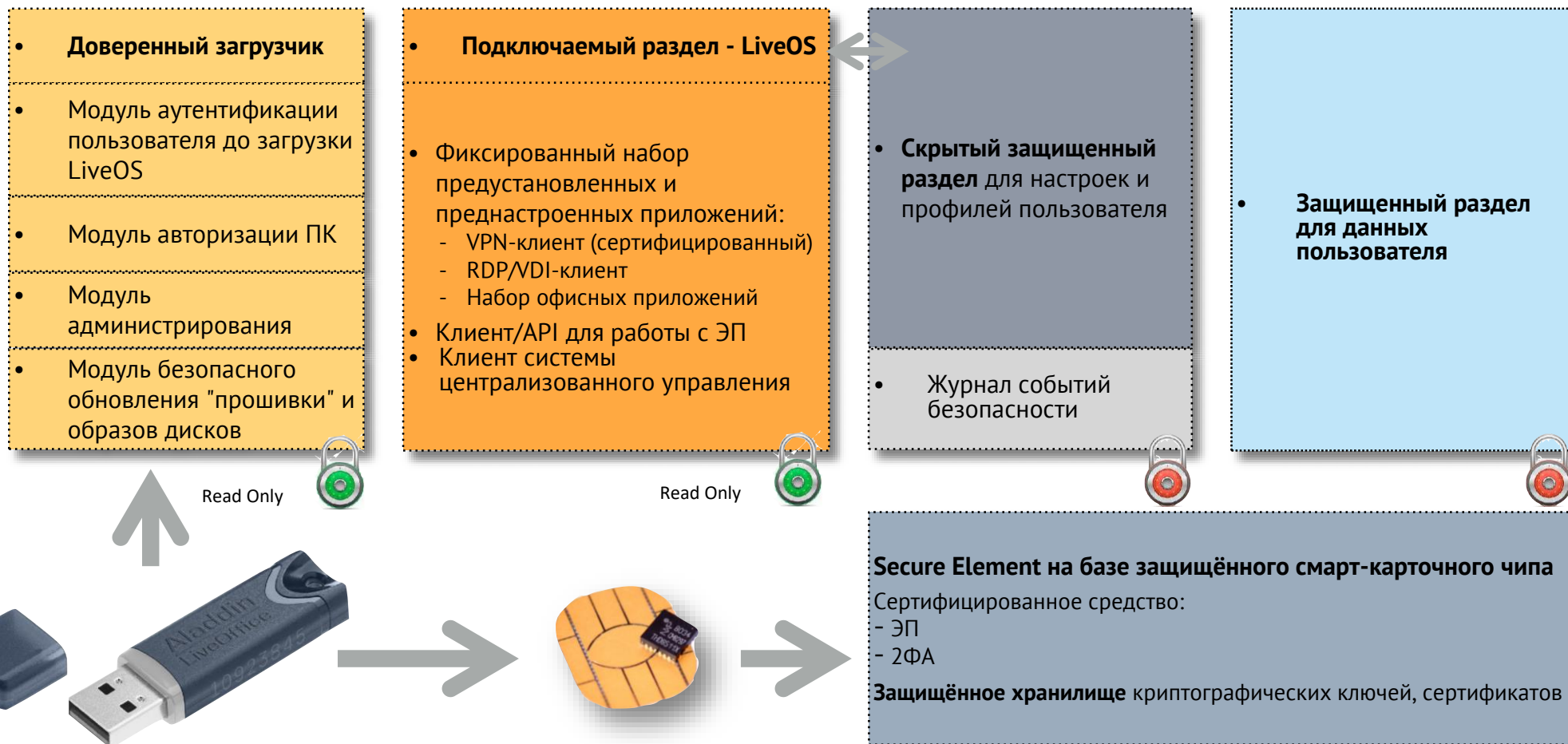
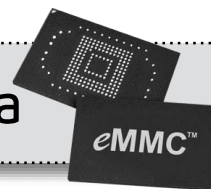
Как обеспечивается безопасность



- Безопасная архитектура устройства (по УД-2)
 - Взаимная аутентификация активных эл. компонентов
 - Защищённый обмен данными
- Доверенная реализация
 - Заказной (ASIC) микроконтроллер на базе ARM-процессора
 - **Secure Element** на базе смарт-карточного чипа (сертифицированная российская криптография, неизвлекаемые ключи), неклонируемость и защита от взлома
 - "Изолирование" карты памяти, загрузка и контроль прошивки встроенного контроллера
 - APDU-Firewall, работа только по "белым спискам" команд
- Собственная ОС-PB для микроконтроллера
 - Доверенная загрузка для встроенной ОС микроконтроллера
 - Аппаратное шифрование защищённых разделов флеш-памяти
 - Возможность удалённого безопасного обновления ("прошивка" зашифрована и подписана ЭП на ключе устройства)
 - Безопасный обмен с ПО на хосте (защита команд и данных)
 - Взламывать украденное устройство и пытаться извлечь из него информацию бесполезно - ключи шифрования в нём не хранятся
- Внедрена технология разработки безопасного ПО (ГОСТ Р 56939-2016), автоматизированного тестирования и поиска уязвимостей

Компоненты решения

Логические диски флеш-памяти USB-токена



Соответствие новым требованиям к средствам удалённого доступа

Защищённое специализированное USB-устройство, соответствующее Требованиям к средствам удалённой работы	✓
Аутентификация пользователя ДО загрузки LiveOS	✓
Возможность работы ТОЛЬКО с авторизованных ПК (<10)	✓
Использование сертифицированных LiveOS и VPN	✓
Возможность безопасного удалённого (централизованного) обновления "прошивки" USB-устройства, образов ОС, настроек	✓
Возможность безопасного удалённого администрирования USB-устройства (СКЗИ, СЗИ, LiveOS, VPN, VDI)	✓
Возможность безопасной транспортировки персонализированных USB-устройств с использованием недоверенных каналов (курьеры, почта)	✓
Возможность работы с ЭП (УКЭП) в системах ЭДО	

Это глубоко интегрированное аппаратно-программное решение, а не "конструктор"



Крипто БД: Выполнение требований по защите информации

Категория требований	Защита ГИС (Приказ ФСТЭК №17)	Защита ИСПДН (Приказ ФСТЭК России №21)	Защита КИИ (Приказ ФСТЭК №239)
Идентификация и аутентификация пользователей	ОК	ОК	ОК
Управление учетными записями пользователей	ОК	ОК	ОК
Контроль доступа	ОК	ОК	ОК
Регистрация событий безопасности	ОК	ОК	ОК
Контроль целостности	-	-	ОК
Контроль и предотвращение утечек информации	ОК	-	ОК
Защита машинных носителей	-	ОК	ОК
Анализ защищенности данных	-	ОК	ОК

Средство защиты информации при импортозамещении

Средство криптографической защиты (СКЗИ)

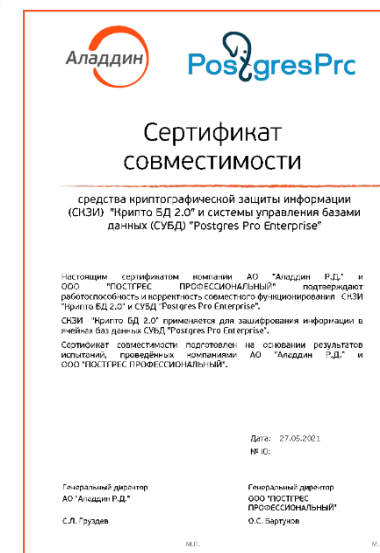
- Соответствует требованиям ГОСТ 28147-89 и ГОСТ 34.12-2018 (шифрование "Магма", "Кузнечик")
- Соответствует требованиям к СКЗИ класса КС1/КС2
- Соответствует требованиям к СКЗИ класса **КС3** (№СФ/124-3472)
- Может использоваться для криптозащиты информации в СУБД

Реестр Минкомсвязи – отечественное ПО

- Решение является полностью отечественной разработкой
- Номер реестра: 509, 518, 4292, 4293

Совместим с PostgresPro

- Подписаны партнерские соглашения
- Оформлен сертификат совместимости



Спасибо!

Будь собой в электронном мире!®



Контакты:

Алекей Сабанов
+7 (985) 924 52 09
a.sabanov@aladdin.ru
www.aladdin-rd.ru

