Методы многофакторной аутентификации и способы их реализации

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

Международные и российские стандарты по аутентификации

<table>
<tr><td>ITU Rec.X.509 (08/1988) Series X: The Directory: authentication framework// ISO/IEC 9594-8</td><td>ГОСТ Р ИСО/МЭК 9594-8-98. Информационная технология. Взаимосвязь открытых систем. Справочник. Ч. 8. Основы аутентификации</td></tr>
<tr><td>ISO/IEC 9798-1:1991. Information technology – Security techniques – Entity authentication mechanisms</td><td rowspan="4">ГОСТ Р 58833-2020. Идентификация и аутентификация. Общие положения

Проект ГОСТ Р XXXXX-202X Идентификация и аутентификация. Уровни доверия аутентификации</td></tr>
<tr><td>ISO/IEC 9798-3:1998. Information technology – Security techniques – Entity authentication – Part 3: Mechanisms using digital signature techniques</td></tr>
<tr><td>ISO/IEC 10181-2:1996. Information technology – Open Systems Interconnection - Security frameworks for open systems – Part 2: Authentication framework</td></tr>
<tr><td>ISO/IEC 29115:2013 Information technology — Security techniques — Entity authentication assurance framework</td></tr>
</table>

Аладдин

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.

Виды аутентификации

- простая;
- усиленная;
- строгая.

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

Аладдин

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.

Аладдин

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 OTP, 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]

Аладдин

Такая разная двухфакторная аутентификация

№	Что используется при аутентификации	Аутентификационная информация	Защита аутентификационной информации	Обмен	Факторы аутентификации	Продукт	Вид аутентификации	Уровень доверия к результату аутентификации
1	многоразовый пароль + устройство OTP	одноразовый пароль + многоразовый пароль	защита многоразового пароля	односторонний	владение + знание	JAS	усиленная	высокий
2	многоразовый пароль + устройство OTP с доступом к устройству по паролю или биометрии	одноразовый пароль + многоразовый пароль	защита устройства и многоразового пароля	односторонний	владение + знание или биометрия	JAS/JMS		
3	устройство (СВТ или смартфон) с криптографическим ПО + доступ к ключу по паролю	криптографические ключи	защита устройства	односторонний или взаимный	владение + знание	JMS + Secure Logon + JaCarta Beyond		
4	СВТ с криптографическим ПО + доступ к ключу по паролю	криптографические ключи	защита ключей	взаимный	владение + знание	JMS + Secure Logon	строгая	очень высокий
5	СВТ с криптографическим ПО и отдельное устройство с помещённым и хранящемся в нём криптографическим ключом + доступ к ключу по паролю или биометрии	криптографические ключи	защита устройства, содержащего ключ	взаимный	владение + знание или биометрия	JMS +Secure Logon		
6	СВТ с криптографическим ПО и отдельное устройство с криптографическим ПО, генерирующее неизвлекаемые ключи (SSCD) + доступ к ключу по паролю и/или биометрии	криптографические ключи	защита устройства, содержащего ключ	взаимный	владение + знание и/или биометрия	JMS		самый высокий

Аладдин

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»

Аладдин

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.

Аладдин

Средства аутентификации

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

Аладдин

Проблемы управления, связанные с аутентификацией

Доступ пользователей

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

Сертификаты, ключевые контейнеры, СКЗИ, etc.

Удостоверяющие центры (Certificate Authority)

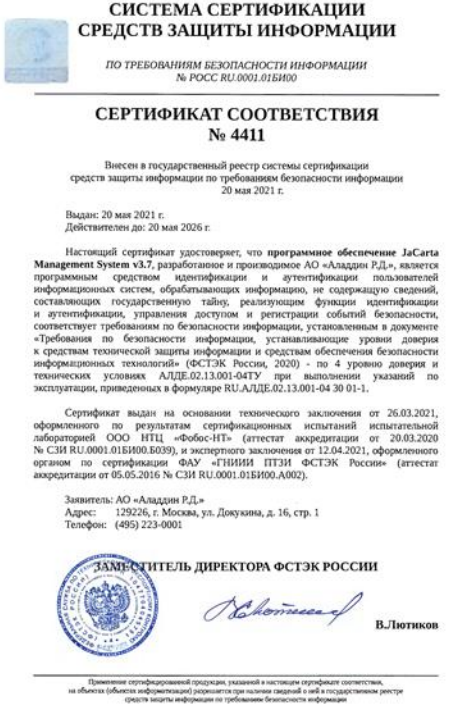
Службы каталогов

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

Аладдин

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 (JAS);
- Сертифицирована ФСТЭК на соответствие УД-4 по требованиям 76 приказа ФСТЭК России.



СИСТЕМА СЕРТИФИКАЦИИ
СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ

ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ СООТВЕТСТВИЯ
№ 4411

Внесен в государственный реестр системы сертификации
средств защиты информации по требованиям безопасности информации
20 мая 2021 г.

Выдан: 20 мая 2021 г.
Действителен до: 20 мая 2026 г.

Настоящий сертификат удостоверяет, что **программное обеспечение JaCarta Management System v3.7**, разработанное и производимое АО «Аладдин Р.Д.», является программным средством идентификации и аутентификации пользователей информационных систем, обрабатывающих информацию, не содержащую сведений, составляющих государственную тайну, реализующим функции идентификации и аутентификации, управления доступом и регистрации событий безопасности, соответствует требованиям по безопасности информации, установленным в документе «Требования по безопасности информации, устанавливающие уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности информационных технологий» (ФСТЭК России, 2020) - по 4 уровню доверия и технических условиях АЛДЕ.02.13.001-04ТУ при выполнении указаний по эксплуатации, приведенных в формуляре RU.АЛДЕ.02.13.001-04 30 01-1.

Сертификат выдан на основании технического заключения от 26.03.2021, оформленного по результатам сертификационных испытаний испытательной лабораторией ООО НТЦ «Фобос-НТ» (аттестат аккредитации от 20.03.2020 № СЗИ RU.0001.01БИ00.Б039), и экспертного заключения от 12.04.2021, оформленного органом по сертификации ФАУ «ГНИИИ ПТЗИ ФСТЭК России» (аттестат аккредитации от 05.05.2016 № СЗИ RU.0001.01БИ00.А002).

Заявитель: АО «Аладдин Р.Д.»
Адрес: 129226, г. Москва, ул. Докукина, д. 16, стр. 1
Телефон: (495) 223-0001

ЗАМЕСТИТЕЛЬ ДИРЕКТОРА ФСТЭК РОССИИ

В.Лютиков

Применение сертифицированной продукции, указанной в настоящем сертификате соответствия, на объектах (объектах информатизации) разрешается при наличии сведений о ней в государственном реестре средств защиты информации по требованиям безопасности информации

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	АРМ
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			
	Крипто Про CSP 5.0	VipNet CSP 4.4	MS Enhanced CSP		

Аладдин

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) . . .

Аладдин

Спасибо!

Будь собой в электронном мире! ®

Контакты:

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

Аладдин