УДК 004.03

Использование стандартов Personal Identity Verification в системах контроля и управления доступом

**Крюков Д.А., Савченко В.В.**

Федеральное государственное бюджетное образовательное учреждение высшего образования «МИРЭА - Российский технологический университет», 119454, Россия, г. Москва, проспект Вернадского, 78, e-mail: vassav96@gmail.com

**Недостаток механизмов стандартизации при внедрении и применении средств контроля и управления доступом зачастую обуславливает уникальность проектов планирования и построения систем контроля и управления доступом (СКУД). Вследствие чего возникает так называемый «вендор-лок» - ситуация, при которой дальнейшее обновление или поддержка СКУД возможны только компанией-поставщиком, изначально установившей СКУД. В статье предлагается универсальная архитектура средств и механизмов аутентификации в СКУД посредством использования открытых стандартов Personal Identity Verification.**

Ключевые слова: информационная безопасность, ИБ, PIV, система контроля и управления доступом, СКУД.

USE OF PERSONAL IDENTITY VERIFICATION STANDARDS IN ACCESS CONTROL AND CONTROL SYSTEMS

**D.A. Kryukov, V.V. Savchenko**

Federal State Educational Institution of Higher Education “MIREA – Russian Technological University” (RTU MIREA), 119454, Russia, Moscow, Vernadscogo avenue, 78, e-mail: vassav96@gmail.com

**The lack of standardization mechanisms in the implementation and application of access control and management tools often determines the uniqueness of planning projects and building access control systems (ACS). As a result, the so-called "vendor-lock" arises - a situation in which further updates or support of the ACS is possible only by the supplier company that originally installed the ACS. The article proposes a universal architecture of means and mechanisms for authentication in ACS through the use of open standards Personal Identity Verification.**

Key words: information security, information security, PIV, access control and management system, access control system.

Система контроля и управления доступом (СКУД) определяется, как совокупность средств контроля и управления доступом, обладающих технической, информационной, программной и эксплуатационной совместимостью [1]. В своей базовой форме система контроля доступа представляют собой систему для контроля доступа сотрудников и посетителей при входе/выходе на объект и в контролируемых внутренних зонах [5].

Система PIV (Personal Identity Verification, Проверка подлинности личности) состоит из компонентов и процессов, которые поддерживают общую платформу (на основе смарт-карт) для аутентификации личности для доступа к различным типам физических и логических сред доступа на предприятии. Спецификации для компонентов PIV способствуют единообразию и функциональной совместимости между различными компонентами системы PIV, между отделами и предприятиями, а также между объектами. Спецификации для процессов представляют собой набор минимальных требований для различных действий, которые необходимо выполнить в рамках действующей системы PIV. При реализации карта PIV поддерживает набор механизмов аутентификации, которые могут последовательно использоваться в разных отделах и/или предприятиях. Аутентифицированная идентификационная информация может затем использоваться в качестве основы для управления доступом в различных физических и логических средах доступа.

Систему PIV можно логически разделить на следующие три основные подсистемы:

– Внешняя подсистема PIV – PIV карты, считыватели карт и биометрических данных, а также устройства ввода PIN-кода. Держатель карты PIV взаимодействует с этими компонентами, чтобы получить физический или логический доступ к нужному ресурсу.

– Подсистема выдачи и управления картами PIV – компоненты, отвечающие за проверку личности и регистрацию, выдачу и управление картами и ключами, а также различные репозитории и службы (например, сетевой справочник PKI, серверы состояния сертификатов), необходимые как часть проверки инфраструктуры.

– Опирающаяся подсистема PIV – физические и логические системы контроля доступа, защищенные ресурсы и данные авторизации. Опирающаяся подсистема PIV становится актуальной, когда карта PIV используется для аутентификации владельца карты, который ищет доступ к физическому или логическому ресурсу [4].

Механизмы аутентификации PIV основаны на взаимодействии пользователя с системой контроля пользователя при помощи средств, схематично представленных на рисунке 1 [5], и включают в себя:

– Аутентификацию с использованием биометрического сравнения вне карты:

а) Несопровождаемую аутентификацию с использованием биометрии (BIO);

б) Сопровождаемую аутентификацию с использованием биометрии (BIO-A);

– Аутентификацию с использованием биометрического сравнения на карте (OCC-AUTH);

– Аутентификацию с использованием асимметричной криптографии:

а) Аутентификация с использованием учетных данных сертификата аутентификации PIV (PKI-AUTH);

б) Аутентификация с использованием учетных данных сертификата аутентификации карты (PKI-CAK);

– Аутентификация с помощью симметричного ключа аутентификации карты (SYM-CAK);

– Аутентификация с использованием уникального идентификатора держателя карты (CHUID);

– Аутентификация с использованием визуальных учетных данных (VIS) [2].

Карта PIV поддерживает набор механизмов аутентификации, которые можно использовать для реализации градуированных уровней доверия для аутентификации личности. Два или более дополняющих механизма аутентификации могут применяться совместно для достижения более высокой степени аутентичности владельца карты PIV. Также механизм аутентификации, который подходит для более высокого уровня доверия, также может применяться для удовлетворения требований для более низкого уровня доверия. Таблица 1 демонстрирует влияние использования различных механизмов аутентификации PIV на количество факторов аутентификации, которые могут быть разделены на «то, что у Вас есть» (Е), «то, что Вы знаете» (З) и «то, кем Вы являетесь» [3].



Рис.1 Взаимодействие пользователя со СКУД

Карта PIV может использоваться для аутентификации личности владельца карты в физической среде контроля доступа. Например, предприятие может иметь охраняемые физические входные двери на пунктах, или может иметь электронные контрольно-пропускных контрольные точки доступа. При выборе подходящих механизмов аутентификации PIV для физического доступа следует использовать подход, основанный на оценке риска. Рекомендуется выбирать механизмы аутентификации на основе защитных зон, установленных вокруг активов или ресурсов.

Для контролируемой зоны - 1, для ограниченной - 2, для закрытой - 3. Подтверждение принадлежности часто бывает достаточным для получения доступа к контролируемой зоне (например, все сотрудники и подрядчики предприятия имеют право доступа к внешнему периметру штаб-квартиры этого предприятия).

Доступ в ограниченные зоны часто основан на функциональных подгруппах или ролях (например, все сотрудники и подрядчики подразделения имеют право доступа к зданию или отделению этого подразделения). Индивидуальное членство в группе или привилегия роли устанавливаются путем установления личности владельца карты. Доступ к закрытым зонам может быть получен только по индивидуальному разрешению.

Таблица 1. Факторы аутентификации механизмов IV

|  |  |  |
| --- | --- | --- |
| Механизмы аутентификации | Факторы аутентификации | Количество факторов аутентификации |
| CHUID + VIS, PKI-CAK, SYM-CAK | Е | 1 |
| BIO | Я | 1 |
| PKI-AUTH (с PIN) | ЕЗ | 2 |
| BIO-A, OCC-AUTH, PKI-AUTH (с OCC) | ЕЯ | 2 |
| PKI-CAK + BIO(-A), SYM-CAK + BIO(-A) | ЕЗЯ | 3 |

Обеспечение аутентификации будет повышено, если СКУД использует соответствующую информацию из предыдущих решений по управлению доступом (так называемый “контекст”) при принятии нового решения по управлению доступом. Например, если владелец карты пытается перейти из контролируемой зоны в ограниченную, СКУД может потребовать, чтобы держателю карты был недавно разрешен доступ в контролируемую зону. Если защитные зоны “вложены” друг в друга, то контекстная аутентификация может быть использована для получения минимального количества факторов аутентификации, требуемых для зоны.

Таблица 2. Всевозможные последовательности механизмов аутентификации PIV

|  |  |  |
| --- | --- | --- |
| Точка доступа 1(контролируемая зона) | Точка доступа 2(ограниченная зона) | Точка доступа 3(закрытая зона) |
| Е | Я или ЕЯ | ЕЗ или ЕЗЯ |
| Е | ЕЗ | ЕЯ или ЕЗЯ |
| Е | ЕЗЯ | ЕЗ, ЕЯ или ЕЗЯ |
| Я | ЕЗ или ЕЗЯ | ЕЗ, ЕЯ или ЕЗЯ |
| Я | ЕЯ | ЕЗ или ЕЗЯ |
| ЕЗ | Я, ЕЯ или ЕЗЯ | ЕЗ, ЕЯ или ЕЗЯ |
| ЕЗ | ЕЗ | ЕЯ или ЕЗЯ |
| ЕЯ | Я или ЕЯ | ЕЗ или ЕЗЯ |
| ЕЯ | ЕЗ или ЕЗЯ | ЕЗ, ЕЯ или ЕЗЯ |
| ЕЗЯ | Я, ЕЗ, ЕЯ или ЕЗЯ | ЕЗ, ЕЯ или ЕЗЯ |

Например, если доступ к ограниченной зоне возможен только из контролируемой зоны, и для доступа к контролируемой зоне требуется аутентификация PKI-CAK, то BIO-аутентификация может использоваться в качестве механизма аутентификации для определения доступа к ограниченной зоне, так как два разных фактора аутентификации «то, что у Вас есть» (Е), и «то, чем Вы являетесь» (Я) используются для предоставления доступа к ограниченной области. Аналогично, если доступ к закрытой зоне возможен только из ограниченной зоны, и для доступа к ограниченной зоне требуется аутентификация BIO, то аутентификация PKI-AUTH (с PIN-кодом) может использоваться в качестве механизма аутентификации для определения доступа к закрытой зоне. Последовательности механизмов аутентификации представлены в таблице 2.

Вместе с тем, карта PIV может использоваться для аутентификации владельца карты при поддержке решений, касающихся доступа к логическим информационным ресурсам. Например, владелец карты может войти в информационную сеть отдела или предприятия, используя карту PIV. Идентификатор, установленный в процессе аутентификации, может использоваться для определения доступа к файловым системам, базам данных и другим службам, доступным в сети.

Таким образом, использование стандартов Personal Identity Verification позволяет определить структуру системы контроля и управления доступом еще до составления договора о внедрении СКУД с поставщиком. Данное утверждение справедливо в том числе для процедуры модернизации СКУД.

Список литературы

1. ГОСТ Р 51241-2008 Средства и системы контроля и управления доступом. Классификация. Общие технические требования. Методы испытаний.

2. A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS). NIST Special Publication 800-116. 2008.

3. Guidelines for the Use of PIV Credentials in Facility Access. NIST Special Publication 800-116 Revision 1. 2018.

4. Personal Identity Verification (PIV) of Federal Employees and Contractors. FIPS PUB 201-2. 2013.

5. Physical Access Control Systems (PACS) Customer Ordering Guide. GSA. 2018.

References

1. GOST R 51241-2008 Access control units and systems. Classification. General technical requirements. Test methods.

2. A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS). NIST Special Publication 800-116. 2008.

3. Guidelines for the Use of PIV Credentials in Facility Access. NIST Special Publication 800-116 Revision 1. 2018.

4. Personal Identity Verification (PIV) of Federal Employees and Contractors. FIPS PUB 201-2. 2013.

5. Physical Access Control Systems (PACS) Customer Ordering Guide. GSA. 2018.