Встроенное ПО с цифровой подписью, режим безопасной загрузки и защита закрытых ключей

Функции кибербезопасности в продуктах Axis

Июль 2020

AXIS COMMUNICATIONS

Содержание

1 Сводная информация

В настоящем документе описываются некоторые функции, доступные в продуктах Axis, которые позволяют снизить риск киберугроз и противодействовать определенным типам атак. К этим функциям относятся следующие:

- встроенное ПО с цифровой подписью
- безопасная загрузка
- доверенный платформенный модуль (TPM)
- Axis Edge Vault с идентификатором устройства Axis.

В число угроз входят следующие:

- взлом встроенного ПО
- взлом встроенного ПО на этапе доставки продукции конечному пользователю
- извлечение закрытых ключей
- несанкционированная замена устройств.

1.1 Встроенное ПО с цифровой подписью

Подписанное встроенное ПО устанавливается поставщиком программного обеспечения, который подписывает образ встроенного ПО с помощью закрытого ключа. Когда у встроенного ПО есть эта закрепленная за ним подпись, устройство будет проверять встроенное ПО перед тем как установить его. Если устройство обнаруживает, что целостность встроенного ПО нарушена, обновление встроенного ПО будет отклонено.

1.2 Безопасная загрузка

Безопасная загрузка представляет собой процесс загрузки, состоящий из неразрывной цепочки криптографически проверенного программного обеспечения, берущей начало в с неизменяемой памяти (загрузочное ПЗУ). В основе безопасной загрузки используется подписанное встроенное ПО и она гарантирует, что устройство будет загружаться только с авторизованным встроенным ПО.

1.3 Доверенный платформенный модуль (TPM)

Доверенный платформенный модуль — это компонент, предоставляющий набор криптографических функций для защиты информации от несанкционированного доступа. Закрытые ключи хранятся в доверенном платформенном модуле и все криптографические операции, требующие использования закрытого ключа, передаются в доверенный платформенный модуль для обработки. Благодаря этому секретная часть сертификата остается защищенной даже в случае взлома. Доверенный платформенный модуль, используемый в отдельных продуктах Axis, сертифицирован в соответствии с требованиями стандарта FIPS 140-2.

1.4 Axis Edge Vault с идентификатором устройства Axis

Новый международный стандарт IEEE 802.1AR описывает процедуру автоматизации и защиты идентификации устройства в сети. В продуктах Axis эти меры обеспечения безопасности реализуются с помощью Axis Edge Vault и идентификатора устройства Axis. Хранилище Edge Vault можно использовать для криптографических задач, выполняемых с надежно хранимыми сертификатами. Закрытая часть сертификатов остается в Edge Vault, даже если она используется. Идентификатор устройства Axis безопасно и постоянно хранится в Edge Vault в качестве сертификата, подписанного корневым сертификатом Axis, и это обеспечивает дополнительный уровень доверия устройства на протяжении всего жизненного цикла изделия.

2 Словарь терминов

Сертификат — в криптографии сертификат представляет собой источник аттестации подписанного документа и свойства пары ключей. Сертификат подписывается центром сертификации (ЦС), и если система доверяет ЦС, она также будет доверять сертификатам, выдаваемым ЦС.

Центр сертификации, ЦС — корень доверия для цепочки сертификатов. Он используется для подтверждения подлинности и достоверности базовых сертификатов.

Federal Information Processing Standards, FIPS — федеральные стандарты по обработке информации. Стандарты шифрования и обеспечения безопасности данных, используемые в США Национальным институтом стандартизации и технологии.

Неизменяемое ПЗУ — применяется для безопасного хранения доверенных открытых ключей и программ, используемых для сравнения подписей, чтобы их нельзя было перезаписывать.

Подготовка — процесс подготовки и оснащения устройства для работы в сети. Этот процесс подразумевает передачу данных конфигурации и настроек политик устройству из центральной точки. Устройство поставляется с ключами и сертификатами.

Криптография открытых ключей — асимметричная криптографическая система, в которой любой пользователь может зашифровать сообщение используя *открытый ключ* получателя, но расшифровать сообщение может только получатель с помощью *закрытого ключа*. Может использоваться как для шифрования, так и для подписывания сообщений.

Transport Layer Security, TLS — безопасность транспортного уровня. Интернет-стандарт для защиты сетевого трафика. TLS отвечает за обеспечение безопасности в протоколе HTTPS.

3 Введение

Компания Axis применяет передовые методики по управлению уязвимостями и реагированию на них в наших продуктах, чтобы свести к минимуму вероятность киберугроз для клиентов. Нет способа гарантировать, что в продуктах и службах не будет дефектов, которые можно использовать для вредоносных атак. Это не относится непосредственно к Axis, а скорее к любым сетевым устройствам. Компания Axis может гарантировать, что она на каждом из возможных этапов всегда прилагает скоординированные усилия по минимизации рисков, связанных с устройствами и службами Axis.

Дополнительные сведения о безопасности устройств и обнаружении уязвимостей см. в разделе *www.axis.com/support/product-security*. Для получения более подробной информации о мерах, которые можно предпринять для снижения рисков влияния распространенных угроз, скачайте руководство по усилению безопасности Axis Hardening Guide на веб-странице *www.axis.com/cybersecurity*.

В этом документе описаны некоторые возможные кибератаки и способы их предотвращения в продуктах Axis. В документе рассказывается, как именно подписывание встроенного ПО и безопасная загрузка могут предотвратить несанкционированный доступ к встроенному ПО и взлом встроенного ПО на этапе доставки продукции конечному пользователю. Кроме того, в документе описывается использование доверенного платформенного модуля (TPM) и Axis Edge Vault, которые можно применять для защиты закрытых ключей. Axis Edge Vault используется для безопасного хранения идентификатора устройства Axis и обеспечивает дополнительный уровень доверия устройства.

4 Обнаружение несанкционированного доступа к встроенному ПО

Одним из возможных направлений атаки, которое злоумышленник может попытаться использовать после других неудачных попыток взлома системы, является попытка заставить владельца системы установить измененные приложения, встроенное ПО или другие программные модули. Измененное программное обеспечение может содержать вредоносный код с определенной целью. Общей рекомендацией является установка программного обеспечения только из доверенных источников. В контексте видеосистемы может существовать «человек посередине», который может изменить встроенное ПО устройства и склонить конечных пользователей установить его. Это непростая задача. Злоумышленник должен быть очень квалифицированным и иметь определенный опыт в этом. Злоумышленнику необходимо очень точно понимать структуру встроенного ПО Axis и как оно работает на устройстве. Тем не менее такие злоумышленники могут существовать, если цена атаки на определенную систему достаточно высока. Общей ответной мерой является использование поставщиком программного обеспечения подписанного ПО.

4.1 Подписывание встроенного ПО

Подписанное встроенное ПО устанавливается поставщиком программного обеспечения, который подписывает образ встроенного ПО с помощью закрытого ключа, хранящегося в тайне. Когда у встроенного ПО есть эта закрепленная за ним подпись, устройство будет проверять встроенное ПО перед тем как установить его. Если устройство обнаруживает, что целостность встроенного ПО нарушена, обновление встроенного ПО будет отклонено.

Процесс подписывания встроенного ПО инициируется путем вычисления криптографического хэш-значения. Затем это значение подписывается закрытым ключом из пары закрытых и открытых ключей, прежде чем подпись будет закреплена за образом встроенного ПО.

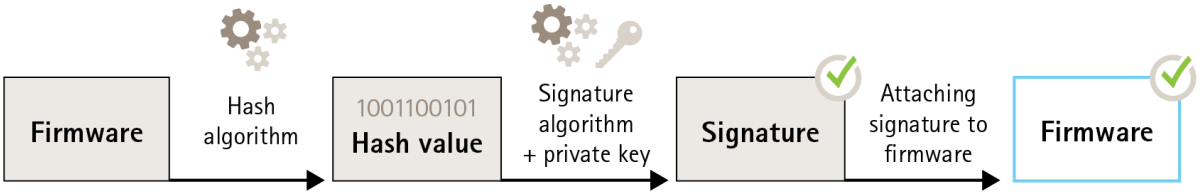

Figure 1. Процесс подписывания встроенного ПО.

Перед обновлением встроенного ПО необходимо проверить новое встроенное ПО. Чтобы удостовериться в том, что новое встроенное ПО не изменено, используется открытый ключ (который входит в состав продукта Axis) для подтверждения того, что хэш-значение было действительно подписано с использованием совпадающего закрытого ключа. Кроме того, при вычислении хэш-значения встроенного ПО и сравнении его с этим проверенным хэш-значением из подписи, может быть проверена целостность встроенного ПО.

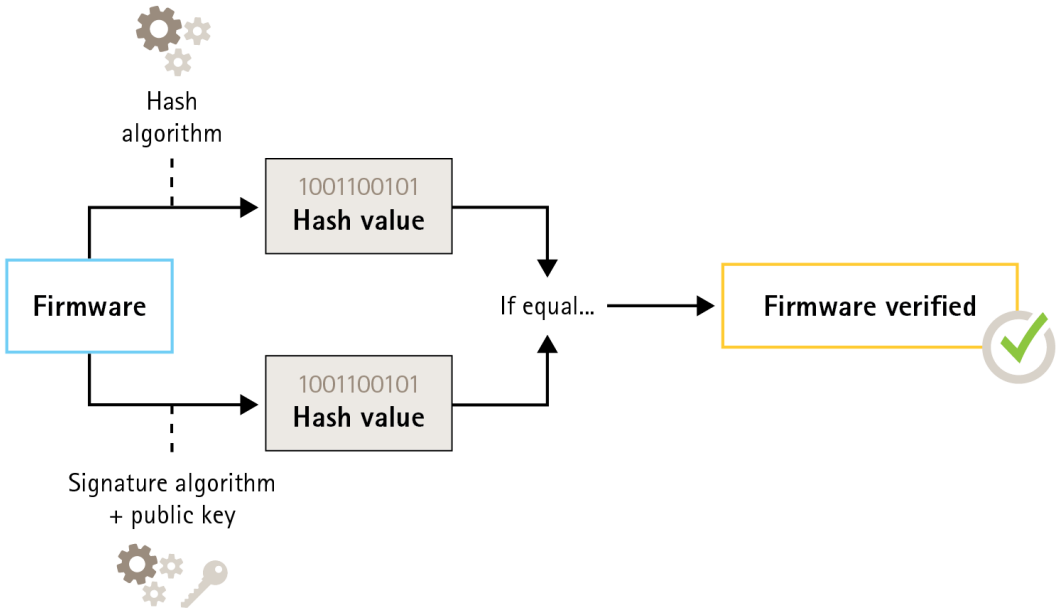

Figure 2. Процесс проверки подписанного встроенного ПО.

4.2 Встроенное ПО с цифровой подписью Axis

Встроенное ПО Axis шифруется с помощью принятого в отрасли способа шифрования с открытым ключом на основе алгоритма RSA. Закрытый ключ хранится в надежно защищенном месте у компании Axis, а открытый ключ встраивается в устройства Axis. Целостность всего образа встроенного ПО обеспечивается за счет использования подписи содержимого образа. Основная подпись проверяет количество дополнительных подписей во время распаковки образа.

5 Защита взлома на этапе доставки продукции конечному пользователю

Подписывание встроенного ПО позволяет защитить устройство (все его последующие обновления встроенного ПО) от установки скомпрометированного встроенного ПО. Но что произойдет, если человек изменит устройство на этапе доставки продукции от поставщика конечному пользователю? Злоумышленник, имеющий физический доступ к устройству во время его доставки, может провести атаку, например, взломать загрузочный раздел устройства, минуя проверку целостности встроенного ПО, чтобы установить измененную вредоносную версию ПО перед тем, как устройство будет развернуто.

5.1 Безопасная загрузка

Безопасная загрузка представляет собой процесс загрузки, состоящий из неразрывной цепочки криптографически проверенного программного обеспечения, берущей начало в с неизменяемой памяти (загрузочное ПЗУ). В основе безопасной загрузки используется подписанное встроенное ПО и она гарантирует, что устройство будет загружаться только с авторизованным встроенным ПО.

Процесс загрузки инициируется загрузочным ПЗУ, выполняющим проверку загрузчика. После этого безопасная загрузка проверяет в режиме реального времени встроенные подписи каждого блока встроенного ПО, загружаемого из флэш-памяти. Загрузочное ПЗУ выступает в качестве корня доверия, и процесс загрузки продолжается до тех пор, пока не будет проверена каждая подпись. Каждая часть цепочки проводит проверку подлинности следующей части, что в конечном итоге приводит к проверке ядра Linux и проверке корневой файловой системы.

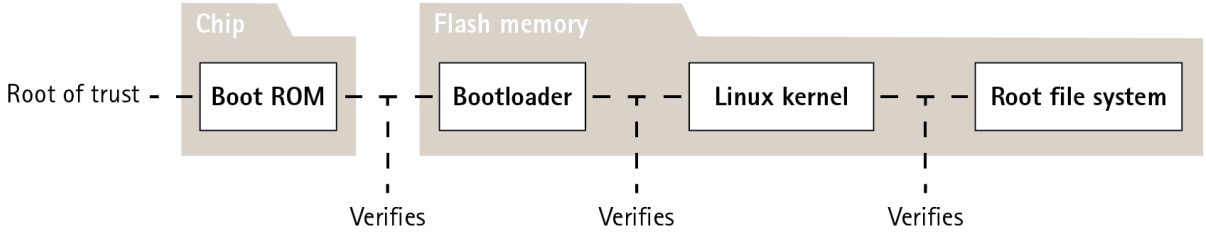

Figure 3. Процесс безопасной загрузки.

5.2 Безопасная загрузка Axis

Во многих устройствах важно, чтобы функциональные возможности низкого уровня нельзя было изменить. Когда другие механизмы обеспечения безопасности устанавливаются поверх программного обеспечения нижнего уровня, безопасная загрузка выступает в качестве безопасного базового уровня, который защищает эти механизмы от обхода.

Для устройства с безопасной загрузкой встроенное ПО, установленное в флэш-памяти, защищено от изменения. Заводской образ по умолчанию защищен, в то время как конфигурация остается незащищенной. Безопасная загрузка гарантирует, что на устройстве Axis не будет возможных вредоносных программ после его сброса до заводских установок.

5.3 Безопасная загрузка и сертификаты для специального встроенного ПО

Несмотря на то что функция безопасной загрузки делает устройство более безопасным, при этом также сужается возможность использования различного встроенного ПО, что усложняет загрузку в устройство любого временного встроенного ПО, такого как встроенное ПО для тестирования или другого специализированного встроенного ПО от компании Axis. Тем не менее компания Axis реализовала механизм, который проверяет отдельные устройства и одобряет использование подобного непроизводственного встроенного ПО. Такое встроенное ПО подписывается другим способом — его одобряют как владелец, так и компания Axis, в результате чего формируется сертификат для специального встроенного ПО. При установке этого ПО на одобренных устройствах сертификат разрешает использование специального встроенного ПО, которое можно запустить только на одобренном устройстве на основе его уникального серийного номера и идентификатора микросхемы. Сертификаты для специального встроенного ПО может создавать только компания Axis, поскольку она является владельцем ключа для подписания таких сертификатов.

6 Безопасность закрытых ключей

Устройства Axis поддерживают протоколы HTTPS (сетевое шифрование) и 802.1X (управление доступом к сети), в которых используется защита транспортного уровня (TLS). Цифровые сертификаты TLS используют пару открытого и закрытого ключей. Закрытый ключ хранится в устройстве, тогда как открытый ключ находится в сертификате. Обратите внимание, что если ни один из протоколов (HTTPS и 802.1X) не используется, ключей для защиты нет.

Злоумышленник может попытаться извлечь из устройства закрытый ключ и сертификат и установить их на атакующий компьютер. В случае с HTTPS этот закрытый ключ можно использовать для перехвата зашифрованного сетевого трафика, передаваемого между устройством и системой управления видео. Либо при спуфинге сети атакующий компьютер может получить доступ к системе управления видео, выдав себя за разрешенное устройство. В случае с 802.1X злоумышленник может использовать закрытый ключ для получения доступа к защищенной по стандарту 802.1X сети, выдавая себя за доверенное устройство.

Сертификаты и закрытые ключи, как правило, хранятся в файловой системе устройства, защищенной политикой доступа к учетным записям и используемой в обычных вычислительных средах. В большинстве случаев это достаточно, поскольку учетную запись взломать нелегко. Следует иметь в виду, что сертификаты могут быть отозваны при подозрении на взлом, что делает закрытый ключ бесполезным.

Некоторые конечные пользователи критически важных систем могут подвергаться повышенному риску злонамеренных действий квалифицированных злоумышленников, которые пытаются взломать

устройство, чтобы извлечь закрытый ключ. Доверенный платформенный модуль (TPM) хранит ключ таким образом, чтобы его невозможно было извлечь даже при взломе устройства.

6.1 Безопасное хранение ключей с помощью TPM (доверенного платформенного модуля)

Доверенный платформенный модуль — это компонент, предоставляющий определенный набор криптографических функций для защиты информации от несанкционированного доступа. Закрытый ключ хранится в доверенном платформенном модуле и никогда не покидает его. Все криптографические операции, требующие использования закрытого ключа, передаются в доверенный платформенный модуль для обработки. Это гарантирует, что секретная часть сертификата никогда не покинет защищенную среду в доверенном платформенном модуле и останется защищенной даже в случае взлома.

6.2 Сертификация FIPS 140-2

К некоторым продуктам и вариантам использования может применяться нормативное требование использовать доверенный платформенный модуль для защиты информации, в некоторых случаях в сочетании с требованием соответствия стандарту FIPS 140-2. FIPS (федеральный стандарт по обработке информации) 140-2 — это стандарт информационной безопасности для криптографических модулей, выпущенный Национальным институтом стандартизации и технологии США.

Проверка в испытательной лаборатории, сертифицированной Национальным институтом стандартизации и технологии, гарантирует правильную реализацию системы модулей и криптографии модулей. Вкратце, сертификация подразумевает описание, составление спецификации и проверку криптографических модулей, утвержденных алгоритмов, одобренных режимов работы и проверок включения питания.

Дополнительные сведения о требованиях к сертификации по FIPS 140-2 можно найти на сайте Национального института стандартизации и технологии *https://csrc.nist.gov/projects/cryptographic-module-validation-program/standards*

6.2.1 Сертифицированный доверенный платформенный модуль в продуктах Axis

Доверенный платформенный модуль, используемый в отдельных продуктах Axis, сертифицирован в соответствии с требованиями стандарта FIPS 140-2. Точнее говоря, он сертифицирован в соответствии с уровнем безопасности 2 этого стандарта, то есть доверенный платформенный модуль также соблюдает требования к авторизации на основе ролей и защите от вскрытия, помимо прочих требований.

7 IEEE 802.1AR — проверка устройства с идентификатором устройства Axis

Человек, покупающий сетевое устройство Axis, может вручную проверить его перед использованием. Посредством визуальной проверки устройства и на основе знаний о том, как выглядят продукты Axis, клиент может удостовериться в том, что устройство действительно произведено компанией Axis. Тем не менее такой тип проверки может быть выполнен только человеком, у которого есть физический доступ к устройству. Поэтому при обмене данными с неподготовленным устройством по сети, как можно убедиться в том, что вы обмениваетесь данными с правильным устройством? Как

проверить, что устройство не было несанкционированно заменено? Ни сетевое оборудование, ни программное обеспечение на серверах не могут выполнять физические проверки. В качестве меры обеспечения безопасности первое взаимодействие с устройством должно выполняться в закрытой сети, в которой устройство можно безопасно подготовить.

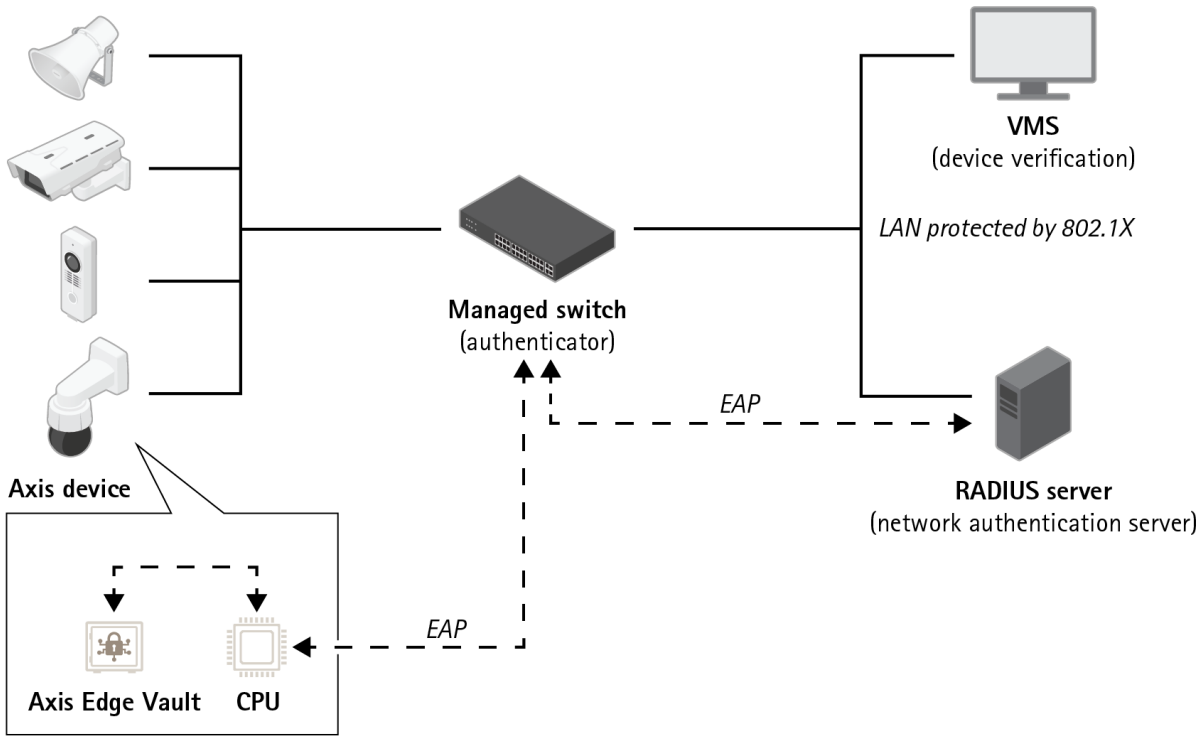

Figure 4. Клиенты могут настроить сервер проверки подлинности на автоматическое принятие в сети приобретенных продуктов Axis на основе серийных номеров устройств и идентификатора устройства Axis.

Новый международный стандарт IEEE 802.1AR (*https://1.ieee802.org/security/802-1ar/*) определяет способ автоматизации и защиты идентификации устройства по сети. Если обмен данными

передается во встроенный защищенный модуль, устройство может вернуть надежный ответ идентификации в соответствии с этим стандартом.

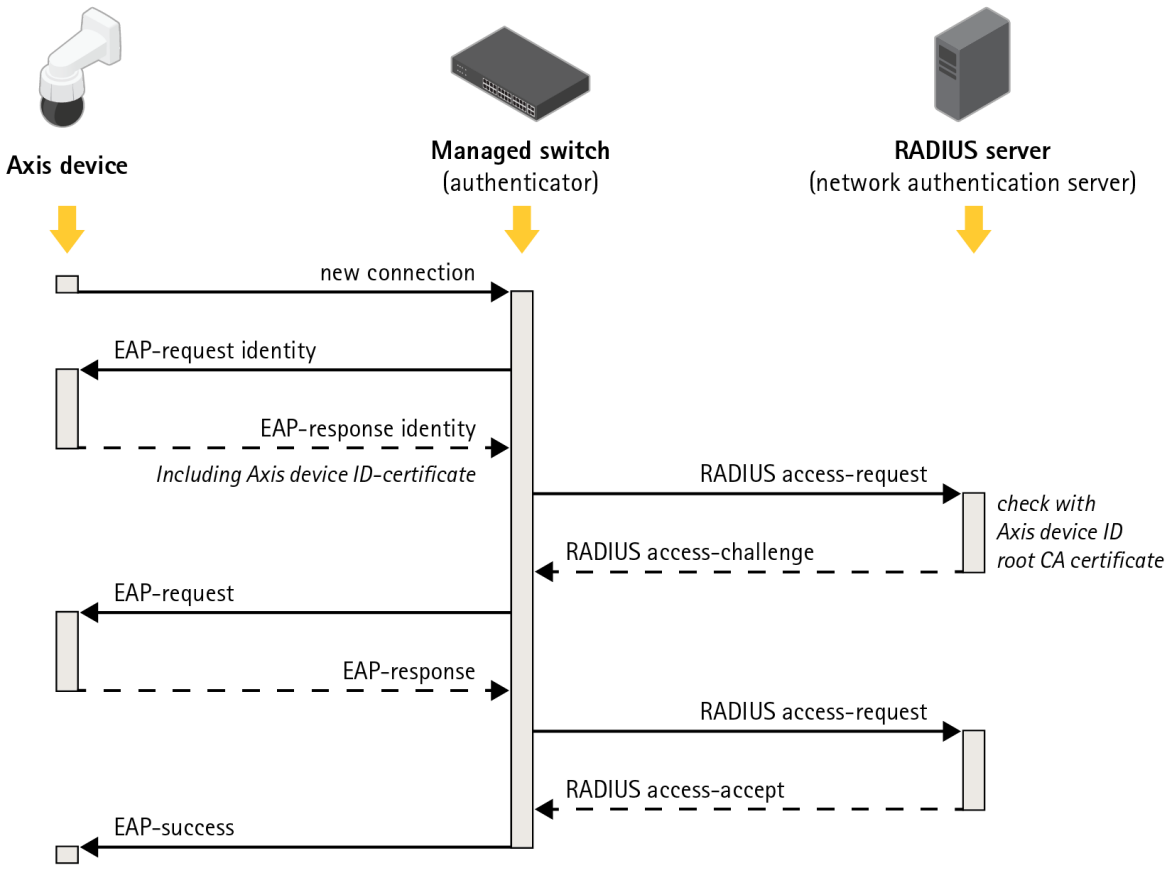

Figure 5. Стандарт IEEE 802.1AR определяет способ идентификации устройства в сети по протоколу, который отправляет запросы протокола расширенной проверки подлинности коммутатору, который, в свою очередь, использует запросы RADIUS (сервиса удаленной аутентификации пользователей) для предоставления доступа.

В продуктах Axis эти меры обеспечения безопасности реализуются с помощью Axis Edge Vault и идентификатора устройства Axis. Axis Edge Vault — это защищенный модуль, в котором установлен идентификатор устройства Axis, то есть набор сертификатов для проверки идентификации устройства. Эти функции предоставляют сети криптографически проверяемое доказательство того, что конкретное устройство было изготовлено Axis и что сетевое подключение к устройству действительно обслуживается тем же самым устройством.

Устройство с идентификатором устройства Axis подготавливается на заводе (с ключами и сертификатами). Эта подготовка позже может быть использована клиентом для дальнейшей подготовки устройства на объекте с другими ключами и (или) сертификатами, позволяя получить доступ к некоторым сетевым ресурсам клиента.

За счет идентификации устройства с помощью идентификатора устройства Axis можно сократить время развертывания устройств, поскольку перед установкой и настройкой устройства в сети необходимо выполнить меньше действий. Другим преимуществом является то, что

идентификатор устройства Axis помимо предоставления дополнительного встроенного источника доверия также предоставляет средства для отслеживания устройств в большой системе.

7.1 Axis Edge Vault

Axis Edge Vault представляет собой защищенный криптографический вычислительный модуль в виде микросхемы, устанавливаемой на печатной плате внутри изделия. В Edge Vault можно безопасного хранить сертификаты и использовать для выполнения криптографических операций с безопасно хранимыми сертификатами.

Сертификаты, хранящиеся в Edge Vault, не должны обязательно покидать его, чтобы устройство могло их использовать. Они безопасно хранятся в Edge Vault даже в том случае, если они используются, так как криптографическое оборудование, работающее с ключом, устанавливается на одной и той же физической микросхеме.

7.2 Идентификатор устройства Axis

Во время производства каждого сетевого устройства Axis «цифровой паспорт» под названием идентификатор устройства Axis безопасно устанавливается в хранилище Axis Edge Vault устройства. Этот идентификатор уникален для каждого устройства и служит для подтверждения его происхождения. Идентификатор устройства Axis представляет собой набор сертификатов, используемых в криптографической операции модуля для подписывания задач, представляемых

встроенным ПО устройства хранилищу Edge Vault. Ответ от этой операции отправляется обратно получателю, который может использовать открытые ключи Axis для проверки подлинности ответа.

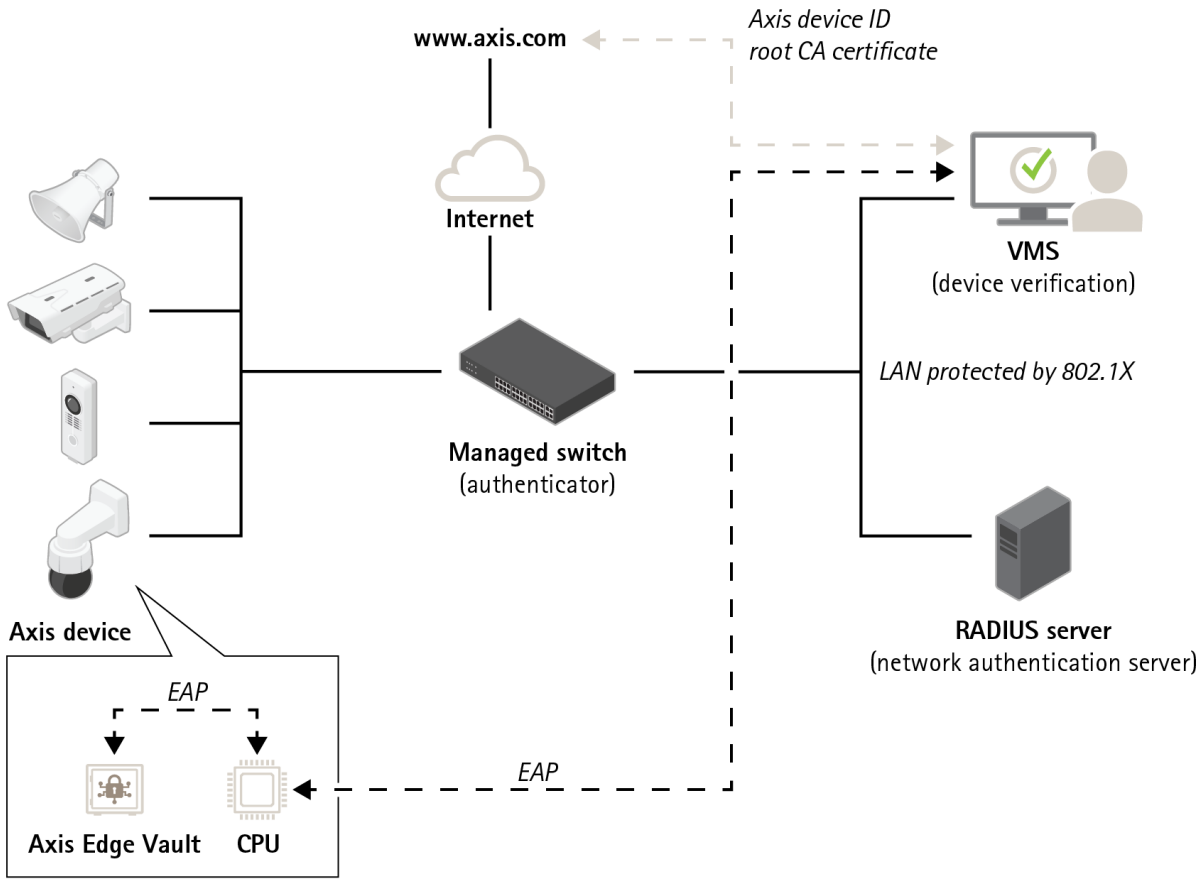

Figure 6. Программные приложения, которые находятся в других частях системы, могут использовать идентификатор устройства Axis и криптографические операции для проверки того, с кем они обмениваются данными. Идентификатор устройства Axis проверяется общедоступным корневым сертификатом ЦС идентификатора устройства Axis, который находится на сайте axis.com.

7.2.1 Иерархии сертификатов

Сертификат представляет собой небольшой фрагмент данных, сочетающий в себе открытый ключ и метаданные, описывающие ключ и подпись от издателя, удостоверяющие достоверность сертификата.

Иерархия сертификатов — это способ удостовериться в том, что сертификат является проверенным. Рассмотрим аналогию между идентификатором устройства Axis и паспортом. Если у вас есть паспорт, правительство вашей страны гарантирует, что вы фактически являетесь человеком, указанным в паспорте. Аналогичным образом все сертификаты идентификаторов устройств Axis заверяются корневым сертификатом ЦС идентификаторов устройств Axis. Так же как и сотрудник таможни доверяет правительству вашей страны в том, что оно правильно выпустило ваш паспорт,

система безопасности сети доверяет корневому сертификату ЦС идентификаторов устройств Axis в том, что она правильно проверяет сертификат Axis подключенного к сети устройства.

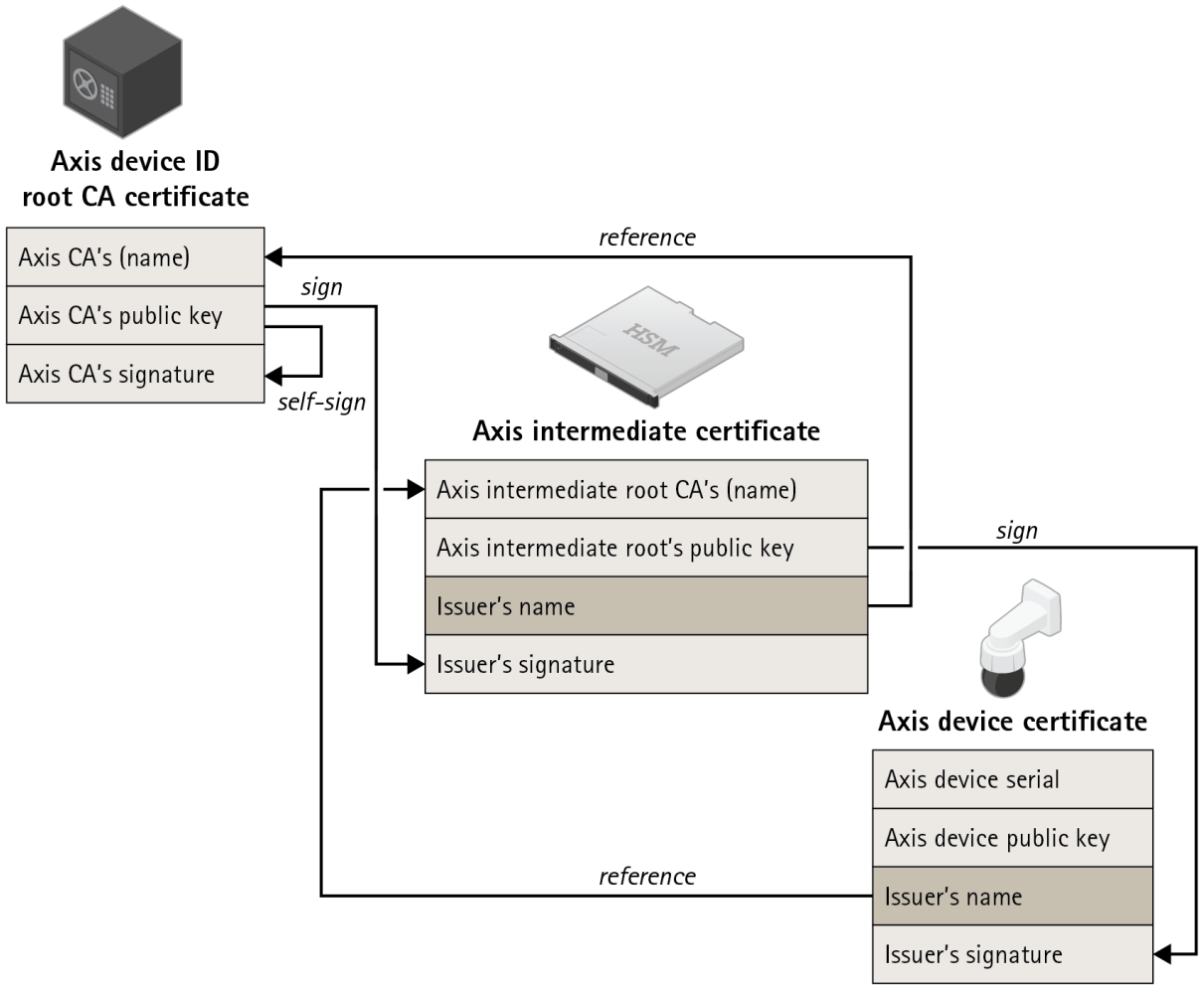

Figure 7. Идентификатор устройства Axis, который является сертификатом, включающим в себя серийный номер изделия, подписывается промежуточным сертификатом, подписанным корневым сертификатом Axis. Поскольку корневой сертификат Axis является очень ценным и его необходимо хранить в безопасном месте, промежуточный сертификат необходим во время подготовки устройства на заводе.

T10154694/RU/M1.8/2007

О компании Axis Communications

Компания Axis вносит весомый вклад в формирование более разумного и безопасного мира, разрабатывая и внедряя сетевые решения, которые не только способствуют повышению безопасности, но и открывают новые пути ведения бизнеса. Занимая в отрасли ведущие позиции, компания Axis поставляет продукцию и оказывает услуги в сфере сетевого охранного видеонаблюдения и аналитики, контроля доступа и звукового сопровождения.

Свыше 3500 специалистов компании Axis трудятся более чем в 50 странах мира, вместе с нашими партнерами разрабатывая и внедряя решения стоящих перед нашими клиентами задач. Компания Axis была основана в 1984 году, Штаб – квартира компании находится в городе Лунд, Швеция.

Для ознакомления с подробной информацией о компании Axis посетите наш веб-сайт *axis.com*