ТЕХНИЧЕСКИЙ ОБЗОР

Функции кибербезопасности в продуктах Axis

— встроенное ПО с цифровой подписью

— безопасная загрузка

— Axis Edge Vault

— Идентификатор устройства Axis

— подписание видео

Ноябрь 2021

AXIS COMMUNICATIONS

Содержание

1 **Краткая информация** 3

1.1 Встроенное ПО с цифровой подписью 3

1.2 Безопасная загрузка 3

1.3 Axis Edge Vault 3

1.4 идентификатор устройства Axis 4

1.5 Подписание видео 4

2 **Словарь терминов** 4

3 **Введение** 5

4 **Обнаружение несанкционированного доступа к встроенному ПО** 5

4.1 Подписывание встроенного ПО 5

4.2 Встроенное ПО с цифровой подписью Axis 7

5 **Защита от взлома на этапе поставки продукции конечному пользователю** 7

5.1 Безопасная загрузка 7

5.2 Безопасная загрузка Axis 8

5.3 Безопасная загрузка и сертификаты для специального встроенного ПО 8

6 **Защита секретных ключей от вмешательства** 8

6.1 Идентификатор устройства Axis 8

7 **Защищенное хранилище ключей** 9

7.1 Безопасное хранение сертификатов в Axis Edge Vault 10

7.2 Безопасное хранение ключей с помощью TPM 10

7.3 Сертификация FIPS 140-2 10

8 **IEEE 802.1AR — проверка устройства с идентификатором устройства Axis** 11

9 **Обнаружение вмешательства в видео** 14

9.1 Подписание видео 14

1 Краткая 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
- защищенная загрузка
- Axis Edge Vault
- идентификатор устройства Axis
- подписание видео.

В число предотвращаемых угроз входят следующие:

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

1.1 Встроенное ПО с цифровой подписью

Подписанное встроенное ПО устанавливается поставщиком программного обеспечения, который подписывает образ встроенного ПО с помощью закрытого ключа. Если у встроенного ПО есть такая присоединенная подпись, устройство проверяет с ее помощью встроенное ПО, прежде чем устанавливать его. Если устройство обнаруживает, что целостность встроенного ПО нарушена, обновление встроенного ПО отклоняется.

1.2 Безопасная загрузка

Безопасная загрузка представляет собой процесс загрузки, состоящий из неразрывной цепочки криптографически проверенного программного обеспечения, берущей начало в неизменяемой памяти (загрузочное ПЗУ). Безопасная загрузка основана на использовании подписанного встроенного ПО; эта технология гарантирует, что устройство способно загружаться только с авторизованным встроенным ПО.

1.3 Axis Edge Vault

Axis Edge Vault - это защищенный криптографический вычислительный модуль, позволяющий выполнять криптографические операции с хранящимися в защищенном хранилище сертификатами. Edge Vault обеспечивает защищенное от вмешательства хранение секретных ключей в устройстве. Эта технология служит основой для реализации более продвинутых функций безопасности.

1.4 идентификатор устройства Axis

Идентификатор устройства Axis работает как уникальное для каждого устройства цифровое удостоверение. Он безопасным и неудаляемым образом сохраняется в Edge Vault в виде сертификата, подписанного корневым сертификатом Axis. Идентификатор устройства Axis служит доказательством происхождения устройства, обеспечивая принципиально новый уровень доверия к устройству на протяжении всего его жизненного цикла.

1.5 Подписание видео

Подписание видео позволяет подтвердить неизменность видео, не подтверждая каждый шаг происхождения видеофайла. В каждой камере в Axis Edge Vault безопасно хранится уникальный идентификатор устройства Axis, который добавляется в подпись при подписании видеопотока. При воспроизведении видео программа просмотра показывает, является ли видео сохранным. Таким образом, подписание видео позволяет отследить происхождение видео до исходной камеры и подтвердить, что оно не было искажено после извлечения из камеры.

2 Словарь терминов

Сертификат — в криптографии сертификатом называют подписанный документ, удостоверяющий происхождение и свойства пары ключей. Сертификат подписывается центром сертификации (ЦС), и если система доверяет ЦС, она также доверяет сертификатам, которые этот ЦС выдал.

Центр сертификации (ЦС) — это корень доверия для цепочки сертификатов. Он обеспечивает подтверждение подлинности и достоверности базовых сертификатов.

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

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

Инициализация — процесс подготовки и оснащения устройства для работы в сети. Этот процесс предусматривает получение устройством данных конфигурации и настроек политик из центрального источника. Устройство поставляется с ключами и сертификатами.

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

TLS – Transport Layer Security, Интернет-стандарт защиты сетевого трафика. TLS обеспечивает безопасность (S - безопасность) в стандарте HTTPS.

3 Введение

Axis применяет передовые методики по управлению уязвимостями в своих продуктах и реагированию на них, чтобы свести к минимуму вероятность киберугроз для клиентов. Нет способа гарантировать, что в продуктах и службах не будет дефектов, которые можно было бы использовать для вредоносных атак. Это относится не только к продукции Axis, но и к любым сетевым устройствам. Что, однако, Axis может гарантировать, - это то, что на каждом из возможных этапов мы прилагаем скоординированные усилия по минимизации рисков, связанных с устройствами и службами Axis.

Подробнее о безопасности продукции и обнаруженных уязвимостях можно прочесть на странице *www.axis.com/support/product-security*. Чтобы подробнее узнать о мерах, которые можно принять для снижения рисков распространенных угроз, загрузите Руководство Axis по укреплению безопасности на указанной выше странице.

В этом техническом обзоре описаны некоторые возможные кибератаки и способы их предотвращения в продуктах Axis. В документе рассказывается, как именно подписывание встроенного ПО и безопасная загрузка помогают 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. Технология Axis Edge Vault используется для безопасного хранения идентификатора устройства Axis и обеспечивает дополнительный уровень доверия устройству. Axis Edge Vault и идентификатор устройства Axis также позволяют реализовать подписание видео, защищающее видеоматериал от подделки после его скачивания из камеры.

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 определенного назначения. Общая рекомендация состоит в том, чтобы устанавливать программное обеспечение только из доверенных источников. В контексте видеосистемы можно представить себе злоумышленника, который мог бы изменить встроенное ПО устройства и склонить конечных пользователей установить его. Это непростая задача, требующая высокой квалификации и настойчивости. Злоумышленнику необходимо очень точно понимать структуру встроенного ПО Axis и его работу на устройстве. Тем не менее такие злоумышленники могут возникнуть, если экономическая выгода от атаки на определенную систему достаточно высока. Стандартная ответная мера состоит в использовании поставщиком программного обеспечения подписанного ПО.

4.1 Подписывание встроенного ПО

Подписанное встроенное ПО создается поставщиком программного обеспечения, который подписывает образ встроенного ПО с помощью хранящегося в тайне закрытого ключа. Если у встроенного ПО есть такая присоединенная подпись, устройство проверяет с ее помощью встроенное ПО, прежде чем устанавливать его. Если устройство обнаруживает, что целостность встроенного ПО нарушена, обновление встроенного ПО отклоняется.

Процесс подписывания встроенного ПО инициируется путем вычисления значения криптографического хеша. Затем это значение подписывается закрытым ключом из пары закрытого и открытого ключей, после чего подпись присоединяется к образу встроенного ПО.

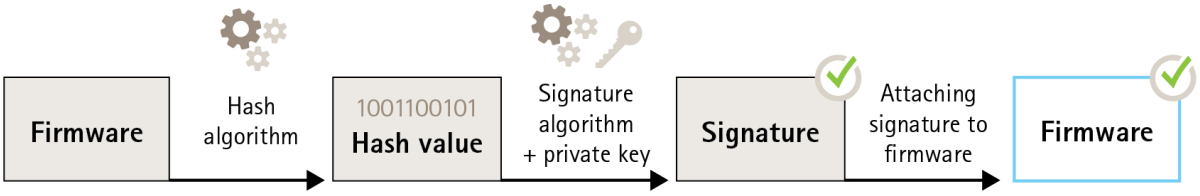

Figure 1. Процесс подписывания встроенного ПО.

Перед обновлением встроенного ПО новое встроенное ПО должно пройти проверку. Чтобы удостовериться в том, что новое встроенное ПО не изменено, с помощью открытого ключа (который входит в состав продукта Axis) проверяется, что значение хеша было действительно подписано с использованием соответствующего закрытого ключа. Далее, вычислив значение хеша встроенного ПО и сравнив его с проверенным значением хеша из подписи, можно быть подтвердить целостность встроенного ПО.

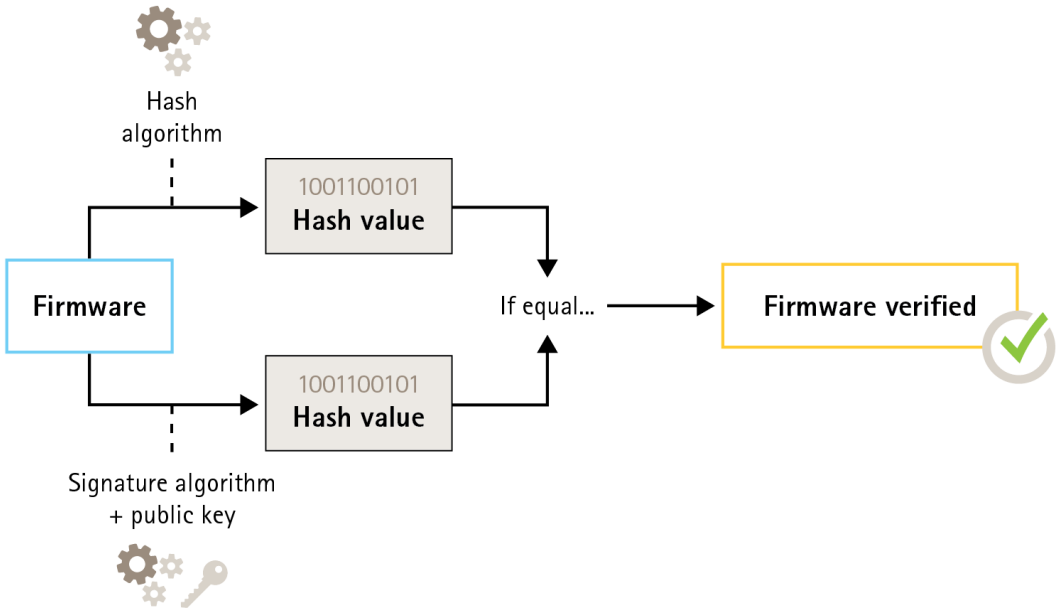

Figure 2. Процесс проверки подписанного встроенного ПО.

4.2 Встроенное ПО с цифровой подписью Axis

Встроенное ПО Axis шифруется с помощью принятого в отрасли 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 подписыванием содержимого образа. Основная подпись подтверждает несколько дополнительных подписей на этапе распаковки образа.

5 Защита от взлома на этапе поставки продукции конечному пользователю

Подписывание встроенного ПО позволяет защитить устройство со всеми последующими обновлениями встроенного ПО от установки скомпрометированного встроенного ПО. Но что произойдет, если некто изменит устройство на этапе доставки продукции от поставщика конечному пользователю? Злоумышленник, имеющий физический доступ к устройству во время его доставки, мог бы 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 неизменяемой памяти (загрузочное ПЗУ). Безопасная загрузка основана на использовании подписанного встроенного ПО; эта технология гарантирует, что устройство способно 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 выполняется только при условии, что все подписи успешно проходят проверку. Каждая часть цепочки подтверждает подлинность следующей части, что в конечном итоге приводит к проверенному ядру Linux и проверенной корневой файловой системе.

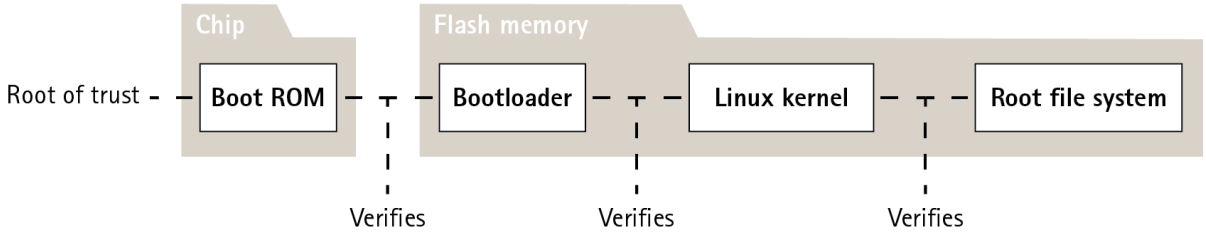

Figure 3. Процесс безопасной загрузки.

5.2 Безопасная загрузка Axis

Для многих устройств важно, чтобы их низкоуровневые функциональные возможности нельзя было изменить. Когда другие механизмы обеспечения безопасности строятся поверх программного обеспечения нижнего уровня, безопасная загрузка выступает в качестве безопасного базового уровня, который защищает эти механизмы от обхода.

В устройствах 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 отсутствие вредоносных программ на устройстве Axis после его сброса до заводского состояния.

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 временного встроенного ПО, например, встроенного ПО для тестирования или другого специального встроенного ПО от компании Axis. Однако Axis реализовала механизм, который позволяет одобрить использование подобного непроизводственного встроенного ПО в конкретных устройствах. Такое встроенное ПО подписывается другим способом, с одобрения как владельца, так и Axis, в результате чего формируется сертификат для специального встроенного ПО. При установке в одобренных устройствах такой сертификат позволяет использовать специальное встроенное ПО, которое может работать только на конкретном устройстве с определенным серийным номером и идентификатором чипа. Сертификаты специального встроенного ПО может создавать только Axis, поскольку только у Axis есть ключ для их подписания.

6 Защита секретных ключей от вмешательства

Одно из главных требований к любой защищенной распределенной системе - это возможность проверки соединения и предотвращения прослушивания. Для этого необходимо, чтобы секретные ключи в каждом устройстве хранились в защищенном от вмешательства хранилище. Axis Edge Vault является именно таким хранилищем и служит основой для реализации более продвинутых функций безопасности.

6.1 Идентификатор устройства Axis

Во время производства каждого сетевого устройства Axis в хранилище Axis Edge Vault устройства безопасно устанавливается «цифровой паспорт» - идентификатор устройства Axis. Этот идентификатор уникален для каждого устройства и служит для подтверждения его происхождения. Идентификатор устройства Axis представляет собой набор сертификатов, используемых криптографической частью модуля для подписывания запросов, которые встроенное ПО устройства передает в хранилище Edge Vault. Полученный в результате этой операции ответ отправляется обратно получателю, который может с помощью открытых ключей Axis проверить подлинность ответа.

Сертификат представляет собой небольшой блок данных, в котором находятся открытый ключ, метаданные, описывающие ключ, и подпись издателя, удостоверяющая действительность сертификата. Иерархия сертификатов дает способ проверить происхождение сертификата.

Рассмотрим аналогию между идентификатором устройства Axis и паспортом. Если у вас есть паспорт, правительство вашей страны гарантирует, что вы действительно являетесь тем лицом, на

чье имя выдан паспорт. Аналогичным образом все сертификаты идентификаторов устройств Axis заверяются корневым сертификатом ЦС идентификаторов устройств Axis. Подобно тому, как сотрудник пограничной службы 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 сертификат Axis подключенного к сети устройства был надлежащим образом проверен.

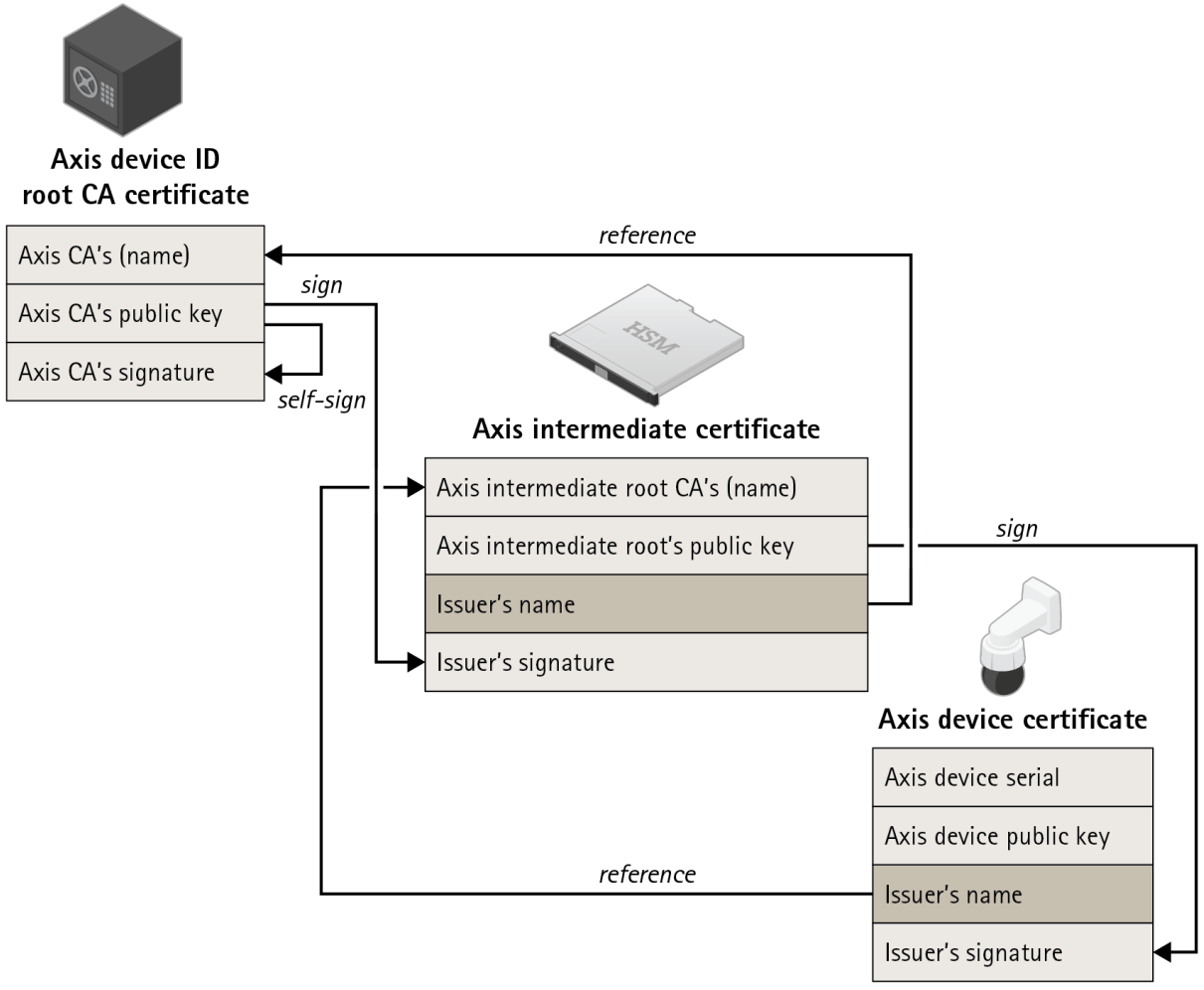

Figure 4. Идентификатор устройства Axis представляет собой сертификат, содержащий в себе серийный номер изделия. Он подписывается промежуточным сертификатом, подписанным корневым сертификатом Axis. При инициализации устройства на заводе используется промежуточный сертификат, поскольку корневой сертификат Axis представляет большую ценность и хранится в особо защищенном месте.

7 Защищенное хранилище ключей

Устройства Axis поддерживают протоколы HTTPS (сетевое шифрование) и 802.1X (управление доступом к сети), в которых используется протокол TLS. Цифровые сертификаты TLS используют пару из 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, защита каких-либо ключей не требуются.

Злоумышленник может попытаться извлечь из устройства закрытый ключ и сертификат и установить их на атакующий компьютер. В случае HTTPS этот закрытый ключ можно было бы использовать для прослушивания шифрованного сетевого трафика между устройством и системой управления видео. Или же атакующий компьютер мог бы внедриться в сеть под видом уполномоченного устройства и получить доступ к системе управления видео. В случае 802.1X злоумышленник мог бы 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 на базе учетных записей и используемой в обычной вычислительной среде. 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 быть подвержены повышенному риску злонамеренных действий квалифицированных злоумышленников, которые пытаются взломать устройство, чтобы извлечь закрытый ключ. Axis Edge Vault позволяет хранить ключи таким образом, что их практически невозможно извлечь даже при получении несанкционированного доступа к устройству.

7.1 Безопасное хранение сертификатов в 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 выполнять криптографические операции с их использованием.

Устройство может использовать хранящиеся в Edge Vault сертификаты, не извлекая их из безопасного хранилища. Они безопасно хранятся в Edge Vault даже тогда, когда они используются, поскольку криптографические вычислительные средства, работающие с ключом, располагается с ними на одном физическом чипе.

7.2 Безопасное хранение ключей с помощью TPM

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

7.3 Сертификация FIPS 140-2

Для некоторых продуктов и вариантов применения требование наличия модуля TPM для защиты информации может быть установлено законом, иногда в сочетании с требованием соответствия FIPS 140-2. FIPS (Federal Information Processing Standard) 140-2 - это стандарт информационной безопасности для криптографических модулей, выпущенный Национальным институтом стандартов и технологий США (NIST).

Проверка в испытательной лаборатории, сертифицированной NIST, гарантирует правильную реализацию системы и криптографии в модуле. Коротко говоря, сертификация подразумевает

описание, составление спецификации и проверку криптографических модулей, утвержденных алгоритмов, одобренных режимов работы и проверок при включении питания.

Подробнее о требованиях сертификации FIPS 140-2 можно узнать на сайте NIST *www.nist.gov*

7.3.1 Сертифицированный доверенный платформенный модуль (TPM) в продуктах Axis

Модуль TPM, используемый в ряде моделей Axis, сертифицирован на соответствие требованиям FIPS 140-2. Конкретно говоря, он сертифицирован на соответствие уровню безопасности 2 этого стандарта, что означает, что TPM соответствует, среди прочего, требованиям авторизации по ролям и подтверждения вмешательства.

8 IEEE 802.1AR — проверка устройства с идентификатором устройства Axis

Покупатель сетевого устройства Axis может вручную проверить его перед использованием. Визуально проверив устройство и на основе знаний о том, как выглядят продукты Axis, клиент может удостовериться в том, что устройство действительно произведено компанией Axis. Тем не менее такого рода проверка может быть выполнена только человеком, у которого есть физический доступ к устройству. Как тогда убедиться в том, что вы обмениваетесь данными с правильным устройством, если вы общаетесь с неинициализированным устройством по сети? 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 инициализировать.

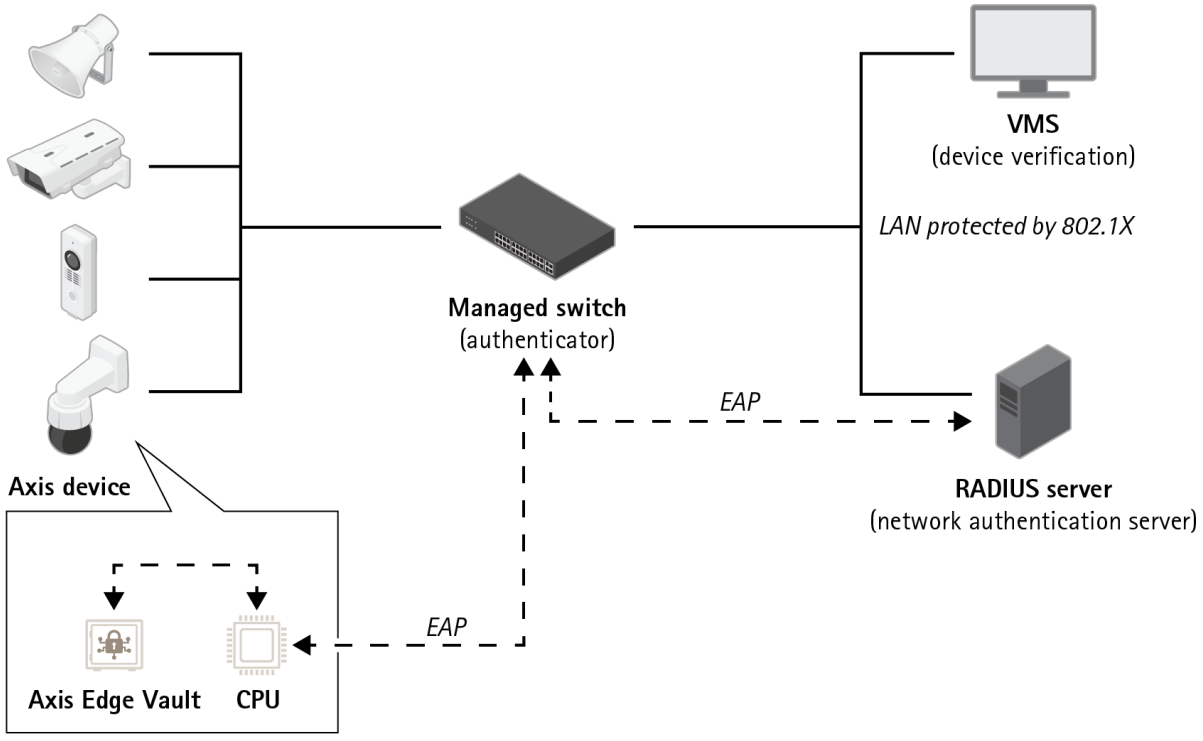

Figure 5. Клиент может настроить сервер проверки подлинности на автоматическое принятие в сети приобретенных продуктов Axis на основе серийных номеров устройств и идентификаторов устройств Axis.

Новый международный стандарт IEEE 802.1AR (*https://1.ieee802.org/security/802-1ar/*) определяет способ автоматизации и обеспечения идентификации устройств по сети. Этот стандарт позволяет

устройству может вернуть надежный ответ идентификации, если обмен данными передается во встроенный защищенный модуль.

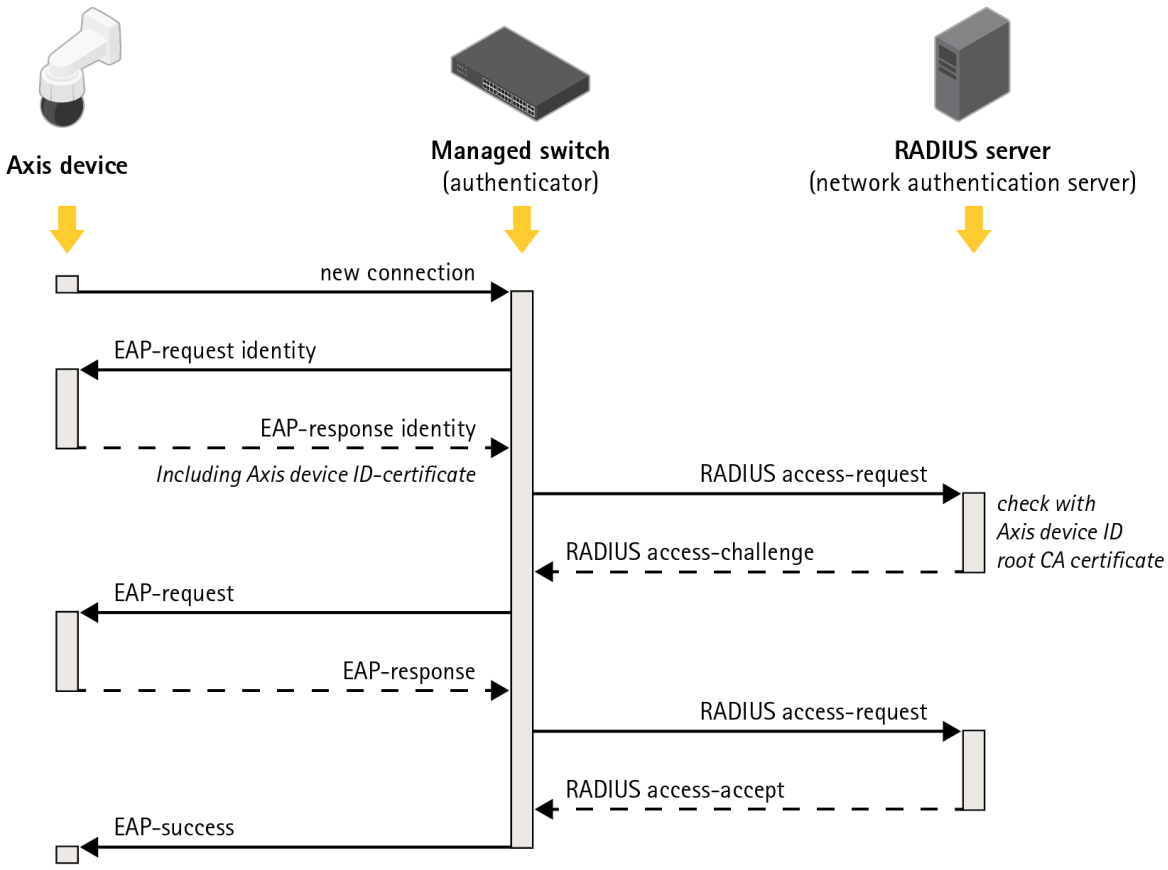

Figure 6. Стандарт IEEE 802.1AR определяет способ идентификации устройства в сети по протоколу, согласно которому устройство отправляет коммутатору запрос EAP (Extensible Authentication Protocol), а коммутатор, в свою очередь, предоставляет доступ, используя запросы RADIUS.

В продукции Axis эти меры безопасности реализуются с помощью технологий Axis Edge Vault и идентификатора устройства Axis. Axis Edge Vault - это защищенный модуль, в котором установлен идентификатор устройства Axis - набор сертификатов, подтверждающих идентификацию устройства. Эти функции предоставляют другим устройствам 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 инициализируется (снабжается ключами и сертификатами) на заводе. Эта инициализация позже может быть использована клиентом для дальнейшей инициализации устройства на объекте, в ходе которой в него добавляются другие ключи и (или) сертификаты, позволяющие получить доступ к определенным сетевым ресурсам клиента.

Идентификация устройств с помощью идентификатора устройства Axis позволяет сократить время развертывания устройств, поскольку перед установкой и настройкой устройства в целевой сети необходимо выполнить меньше действий. Другим преимуществом является то, что

идентификатор устройства Axis не только служит дополнительным встроенным источником доверия, но и предоставляет средства для отслеживания устройств в большой системе.

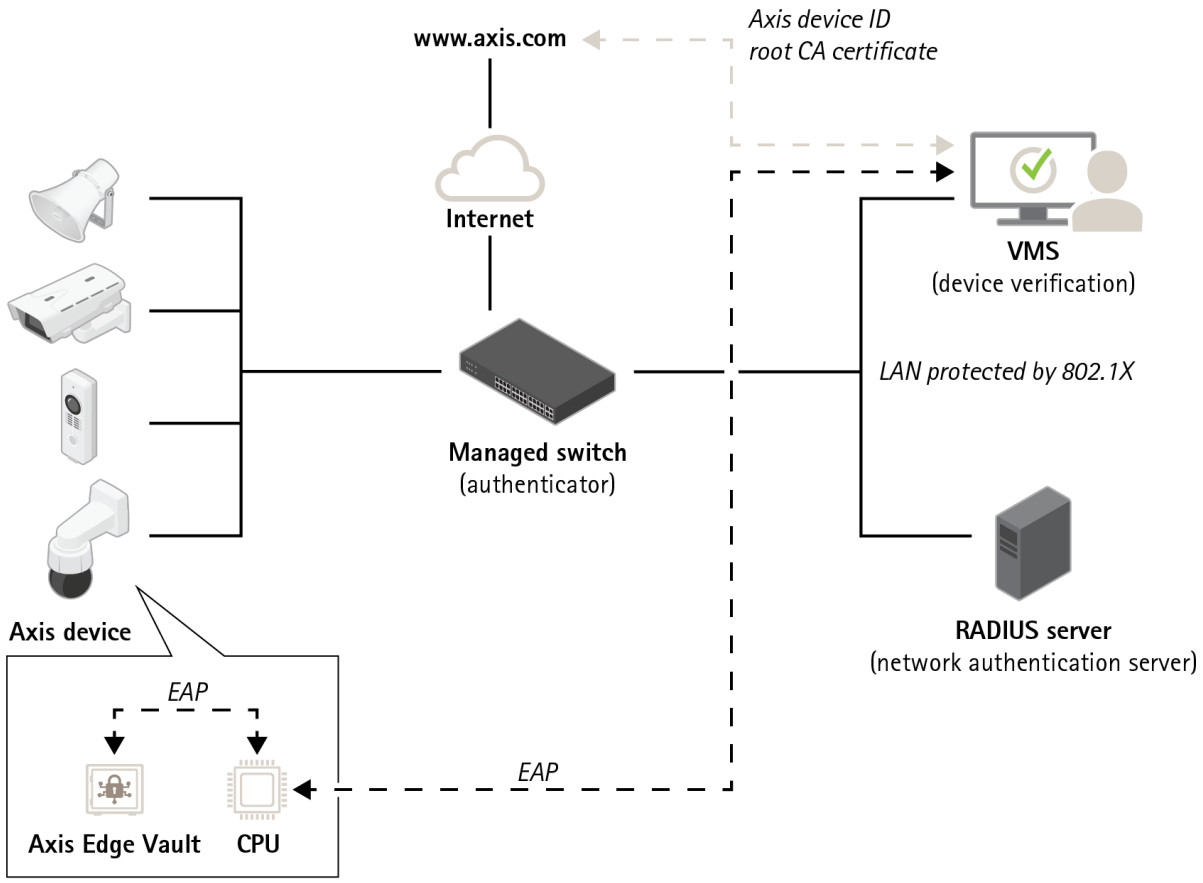

Figure 7. Программные приложения, которые находятся в других частях системы, могут использовать идентификатор устройства Axis и криптографические операции для проверки того, с кем они обмениваются данными. Идентификатор устройства Axis проверяется открытым корневым сертификатом ЦС идентификаторов устройств Axis, который доступен на сайте axis.com.

9 Обнаружение вмешательства в видео

Один из основополагающих принципов отрасли безопасности состоит в том, что видео, записанное камерой видеонаблюдения, является подлинным и заслуживает доверия. Функция подписания видео разработана для сохранения и укрепления доверия к видеозаписям как доказательству. Подтверждая подлинность видео, эта функция позволяет удостовериться, что видео не было отредактировано или сфальсифицировано после его считывания из камеры.

9.1 Подписание видео

Предлагаемая Axis функция подписания видео позволяет защитить видеопоток от искажения и подтвердить происхождение видео с возможностью прослеживания до камеры, которой оно было снято. Это дает возможность доказывать аутентичность видео, не доказывая каждый этап происхождения видеофайла.

Сотрудник полиции может списать экспортированные видеофайлы записанного камерами охранного видеонаблюдения инцидента на USB-накопитель и сохранить их в системе EMS (система управления видеодоказательствами). При экспорте видео из камеры полицейский может удостовериться, что видео надлежащим образом подписано. Если эти видеоматериалы будут впоследствии использоваться в судебном процессе, суд может проверить и подтвердить время, когда видео было записано, какой камерой была сделана запись, и удостовериться, что видеокадры не были изменены и удалены. Эту информацию может проверить в видео любой пользователь, располагающий проигрывателем файлов Axis.

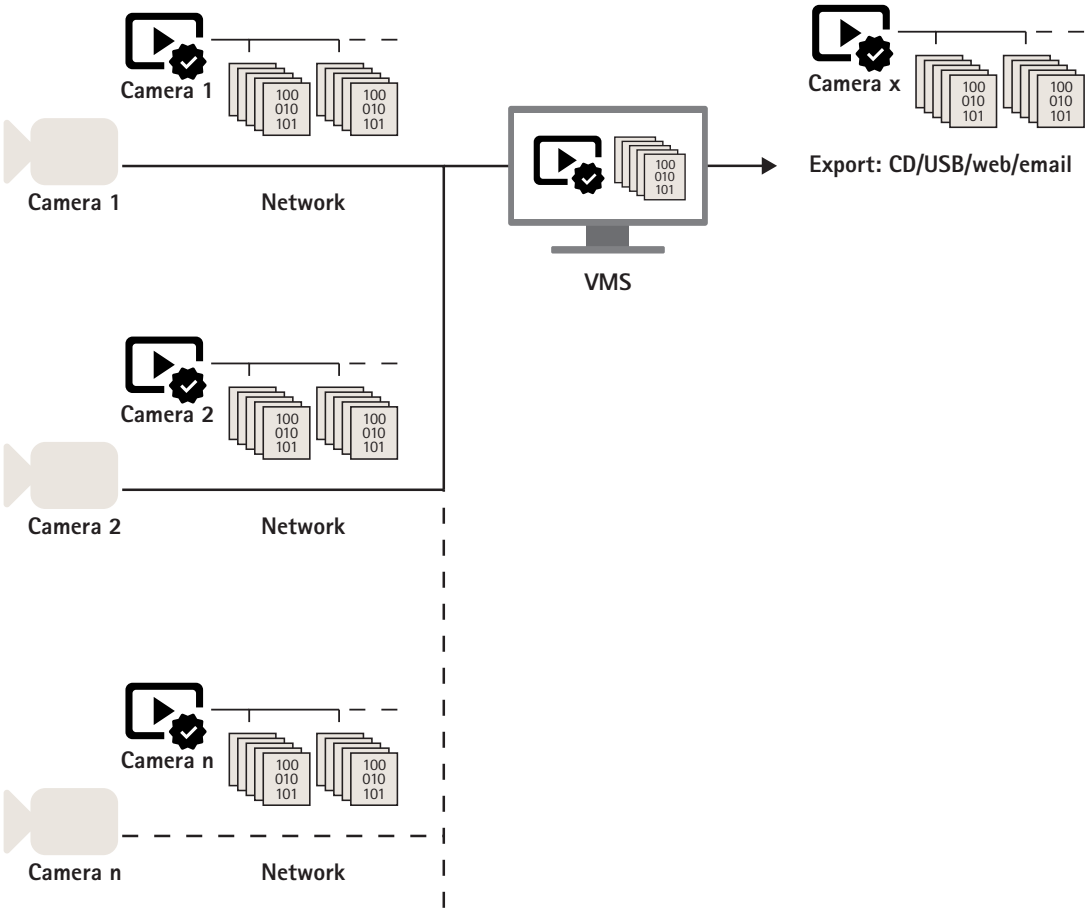

Figure 8. Поскольку подписание видео происходит непосредственно в камере, подлинность его содержимого можно проверить на любом шаге от источника до конечного использования.

Каждая камера имеет в своем Axis Edge Vault уникальный идентификатор устройства, который добавляется в подпись при подписании видеопотока. Это делается путем вычисления хеша каждого

видеокадра, включая метаданные, и подписания этого объединенного хеша в Edge Vault. После этого подпись записывается в видеопоток в специальные поля метаданных (заголовок SEI).

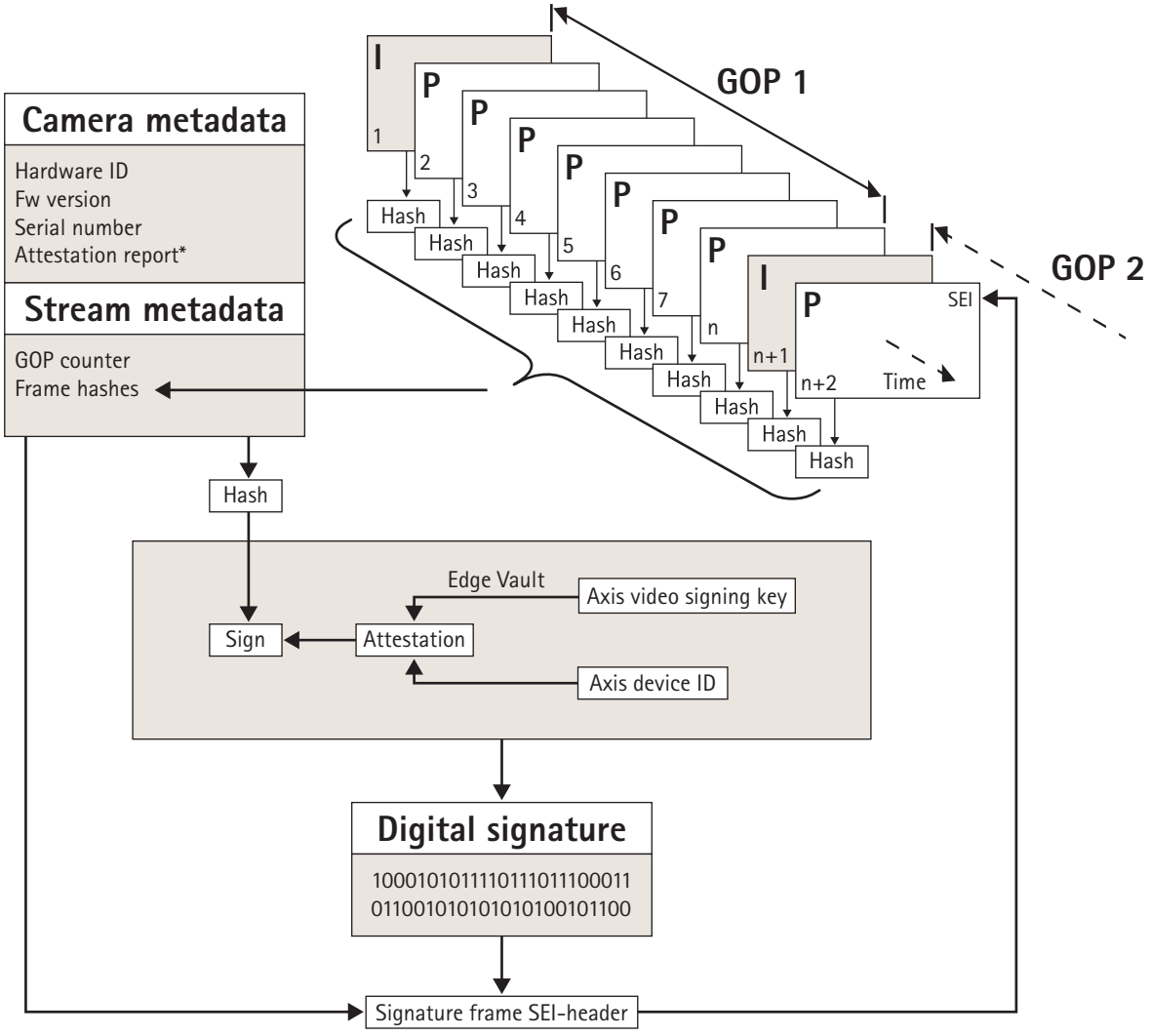

Figure 9. Графическая схема добавления подписи в метаданные видео. Содержимое каждого кадра группы кадров (GOP) хешируется вместе с хешем метаданных камеры и метаданных потока. Полученный в результате хеш GOP подписывается в Edge Vault. После этого подпись и метаданные добавляются в заголовок SEI, передаваемый в потоке.

* *Отчет о подлинности позволяет удостоверить источник и происхождение пары ключей, используемой для подписания. Проверка подлинности ключа позволяет убедиться, что ключ безопасно хранится в аппаратном модуле определенного устройства. Тем самым удостоверяется происхождение видео.*

Само подписание происходит с использованием уникального для каждого устройства ключа подписания видео, привязанного к уникальному для каждого устройства идентификатору устройства Axis. Отчет о подлинности присоединяется к видеопотоку в начале и затем через определенные интервалы, обычно раз в час. Поскольку метаданные содержат хеш

каждого кадра, можно убедиться в правильности каждого конкретного кадра. Чтобы подписание было полным, необходимо защитить структуру групп кадров (GOP) в видео. Это делается путем включения в подпись хеша первого ключевого кадра следующей GOP. Это исключает возможность незаметного вырезания или перестановки кадров. Маловероятные события потери кадров при потоковой передаче или повреждения контента при сохранении будут помечены аналогичным образом.

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, сетевых домофонов и звукового сопровождения. Свыше 3800 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.

Более подробную информацию о компании Axis можно найти на нашем веб-сайте *axis.com*.