Implementing CDSA-Compliant Content Protection and Security Using Microsoft Azure

Microsoft

Abstract

Building secure solutions to protect corporate and user data can be costly for any organization, and face numerous technical challenges along the way. In the media and entertainment industry, these challenges are compounded by the need to create new channels for the creation, distribution, and consumption of high-value digital assets. The Content Delivery and Security Association (CDSA), a worldwide standards body for the entertainment and software industry, has long understood the need of its members to operate individually and jointly in a secure manner, particularly in an enhanced threat landscape that has evolved dramatically. As a result, the CDSA developed the Content Protection & Security (CPS) standard to provide a set of controls designed to ensure the continued integrity of intellectual property, confidentiality, and media asset security at all stages of the supply chain.

Microsoft Azure is the first hyper-scale cloud platform certified to comply with the CDSA's CPS standard, offering powerful and highly scalable cloud-based encoding, encryption, and streaming components to enable the creation and distribution of both internal digital work products as well as the distribution and monetization of valuable and premium digital content to a global audience using today's most popular digital devices.

This document describes how Azure, and in particular Azure Media Services, can enable you to create CDSA CPS compliant solutions securely. Emphasis will be placed on describing how the controls are implemented in Azure to provide CPS-compliant content improved protection and security, and help you understand how Azure helps protect your cloud deployments and determine if these capabilities and controls are suitable for your unique requirements.

NOTE: Certain recommendations contained herein may result in increased data, network, or compute resource usage, and increase your license or subscription costs.

Version 1, Published September 2015

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

Table of Contents

1 Introduction

Many organizations can benefit from using cloud technologies to meet their business goals, which offer scalability, availability, security, and cost effectiveness for global reach. Organizations that have not started using the cloud often believe that their specific workflows cannot be supported by cloud services, or that security and regulatory compliance issues will prevent them from adopting services effectively.

The media industry is exploring the use of cloud computing at a time of profound transformation. Its products, distribution channels, supply chains—even its daily tasks and workflows—are increasingly *digital*. As a result, the industry's driving principals of art and commerce are becoming inextricably tied to vast arrays of routers, servers, networks, and security systems. The media business is therefore becoming as much about the installation, management, and use of IT infrastructure as it is about the creation and consumption of digital assets. The very nature and value of digital products makes it important that media organizations deploy solutions that work in concert to help ensure *data confidentiality*, *integrity*, and *availability*, as well as *accountability* amongst all entities in their global digital supply chain. In addition to handling the basic IT challenges (network and server availability, security, etc.) that every organization deals with, such an infrastructure must also address several industry specific challenges:

- Controlling the distribution of digital work products, i.e. solving the “copy of copies” dilemma
- Using the Internet as a new channel for broadcast and consumption
- Identity (license) management for both end customers and supply chain partners
- Rights management and encryption
- Disaster recovery and availability
- Security management and incident response

When considering cloud solutions, three basic questions arise for any company handling media content:

1. Can it support the usual day-to-day business tasks common to all enterprises, e.g. email security, document management, server management, etc.?
2. Can it support/enable the existing *and* future workflows and distribution challenges that are unique to the media industry?
3. Can the above be done cost-effectively while helping ensure security and compliance with industry standards for creating and archiving content?

There are many cloud providers offering solutions to the first question through Infrastructure as a Service (IaaS) offerings. The challenge for the media industry, particularly as it relates to the second question, is that an IaaS solution is not sufficient. If the most basic rationale for cloud services is to offload the creation of a complete platform (datacenter, hardware, and software) and instead provision a turnkey solution, then pushing the servers and storage to the cloud is only half the battle—the technologies, services, and processes necessary to build and deploy solutions such as on-demand streaming still have to be implemented on top of that now cloud-based infrastructure. Thus, what media companies really need is a *media-centric Platform as a Service (PaaS)*. In other words, the solution is not to relocate the servers, storage, and other infrastructure components to the cloud. The solution is to take advantage of cloud capabilities and controls to create and manage digital assets, deploy broadcast channels, and manage customer access and rights. An offering that combines the infrastructure advantages of cloud computing with the industry-specific capabilities necessary to build secure digital media solutions provides a far more complete solution.

Azure Media Services is a media platform built on top of Azure's infrastructure. It offers powerful and highly scalable cloud-based encoding, encryption, and streaming components to enable the creation and distribution of both pre-production digital work as well as the distribution and monetization of valuable and premium digital content to a global audience using devices such as tablets and mobile phones. Azure is certified to comply with the rigorous Content Protection & Security (CPS) standard developed by the Content Delivery and Security Association (CDSA), a worldwide standards body for the entertainment and software industry. In addition to being the only cloud platform certified by the CDSA, Azure leads the industry in meeting a broad set of international and industry-specific compliance standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2, as well as country-specific standards including Australia CCSL, UK G-Cloud, and Singapore MTCS. Microsoft was also the first to adopt the uniform international code of practice for cloud privacy, ISO 27018, which governs the processing of personal information by cloud service providers. More detailed information about Azure's compliance programs can be found at http://azure.microsoft.com/en-us/support/trust-center/compliance/.

This document describes controls in Azure to provide CPS-compliant content protection and security for your organization's IT requirements, as well as describes how to create, protect, and operate digital media services such as on-demand streaming.

2 Content Protection and Security Standard

The CDSA's CPS standard provides guidance and requirements to secure media assets such as video-on-demand and live streaming broadcasts within a Content Security Management System (CSMS). This standard details a set of controls designed to ensure the continued integrity and confidentiality of intellectual property and media asset protection at all stages of the supply chain. It is organized into seven capability frameworks:

1. Management Controls
2. Personnel and Resources
3. Asset Management
4. Physical Security
5. IT Security
6. Training and Awareness
7. Business Resilience

The requirements define a series of policies, processes and controls designed to assess, manage and minimize risk to an acceptable level. The continued integrity of intellectual property, confidentiality and media asset security can be assured. A more detailed overview of the CPS standard can be found at http://www.cdsaonline.org/wp-content/uploads/2010/06/CPS-Standard-March-2014.pdf.

The Azure Media Services CSMS has been validated by the CDSA, and as a result Microsoft has been awarded certification to this standard. *It is the first and only CPS-certified cloud-based platform for media services.* Microsoft is committed to continuing annual CDSA audits, as well as maintaining internal audits and controls to retain CPS certification. Customers should contact Microsoft Support (or new customers can contact their account representative) to request a copy of the audit report.

3 Azure Overview

This section provides a brief overview of Azure's security model.

3.1 Accounts and Subscriptions

Azure subscriptions help you organize access to your cloud service resources, and contain Compute Services, Data Services, Application Services, and Network Services. Each subscription can have a different billing and payment setup, so you can have different subscription plans.

Access control for managing these services is governed by the subscription. The ability to authenticate with a Microsoft Account or an organizational account associated with the subscription grants full control to all of the services contained within that subscription. This master account can be used to authorize additional accounts that are able to manipulate the subscription.

Subscriptions can be associated with Microsoft Accounts, organizational accounts in Azure Active Directory, or organizational accounts federated from an on-premises Active Directory domain. They can be managed through the Azure Portal Web site or programmatically through the Service Management API (SMAPI) using command-line tools or Visual Studio.

Authentication to the Azure Portal and SMAPI uses OAuth 2.0 tokens generated from credentials associated with the Microsoft Account or organizational account. SMAPI queues requests to the appropriate service (such as Azure Fabric, which is in charge of provisioning, initializing, and managing virtual machines).

The preferred way to access the Azure management portal and most client tools for services (such as Visual Studio or PowerShell) securely is through a token-based account authentication scheme. The lifespan of these tokens can be set as short as a day or a few weeks. However, if you need persistent client access to service management functions—for example, to enable long-running integrated deployment scripts or code projects—then an alternative approach is using certificate-based management. Certificate-based management is more complex and requires a public key infrastructure (PKI). In general, account-based authentication is preferred over certificate-based authentication for service management functions as service accounts can be easier to manage through an identity solution.

For more information on subscriptions and best practices, see https://msdn.microsoft.com/en-us/library/azure/hh531793.aspx

3.2 Compute Services

Azure Compute services consists of Virtual Machines, Cloud Services, and App Services. Guidance on selecting the proper service can be found here.

3.3 Storage Services

Storage services consists of Azure Storage and SQL Databases. Access to storage accounts and SQL Databases by Azure compute services must be explicitly granted by providing appropriate authorization information to that compute service.

Azure Storage provides high-performance access to data that does not require complex searching capabilities.

- Full access to each Azure Storage Account is authorized by proof of possession of a per-storage-account symmetric key called a Storage Access Key (SAK).
- Shared Access Signature (SAS) tokens can be generated using storage access keys to provide more granular, restricted access.
- Storage access keys can be reset via the Azure Portal or SMAPI.

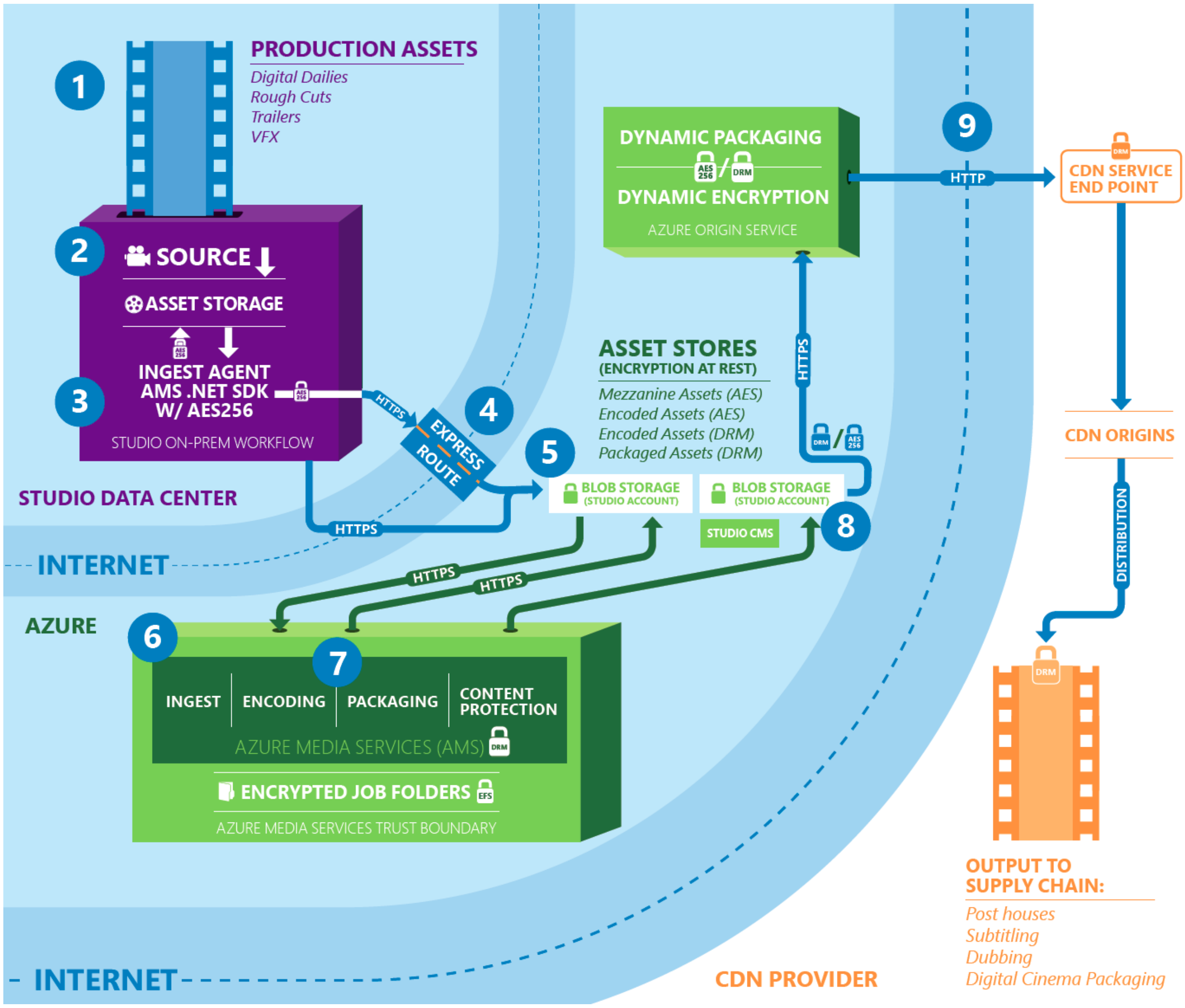
Full access to each SQL Database is authorized by a SQL account with a username and password. The master account password can be reset using the Azure Portal or SMAPI. Other accounts can be created within a SQL Database.

3.4 Network Services

Azure network security can be viewed from three perspectives: encryption, control, and isolation. Additional protection is available by layering partner solutions for application security, such as web application firewalls and intrusion prevention virtual appliances.

Encryption is used at points of data ingress and egress from Azure, when customer data is moved by an Azure service, and for most basic communications by the cloud fabric itself. Management interfaces such as the Azure Portal enforce HTTPS by default, and Azure Media Services employ AES-256 to protect files in-transit, as can be seen in the following table and figure:

STEP	TASK
1	Production creates file-based content
2	Content is temporarily aggregated in the Studio's on-premises asset management repository
3	Studio uses Azure Ingest SDK to encrypt content and prepare for uploading into Azure Media Services, where it will be protected and backed up
4	Studio transmits content via Azure's ExpressRoute, which provides a secure communication channel to Azure Media Services
5	ExpressRoute delivers content into Studio's protected Azure Storage subscription
6	Content is then ingested over encrypted HTTPS channel into Azure Media Services pipeline where it will be protected by Encrypted File Services every step along the way
7	Studio can perform additional content operations such as transcoding, taking full advantage of Azure's chain of custody, change control and privilege management features. At this point the Studio can apply further security beyond file level encryption by applying DRM functionality to restrict viewing and playback features
8	Once content operations are complete, Azure Media Services returns the content securely to Azure Storage
9	Protected content (with optional DRM features) is packaged and delivered to Azure's Content Delivery Network where it can be routed to the Studio's various supply chain partners in post-production or theatrical distribution over an HTTPS encrypted channel



3.5 Service Availability

There are two primary threats to cloud service availability: the failure of devices, such as drives and servers, and the exhaustion of critical resources, such as compute under peak load conditions. Azure provides a combination of resource management, elasticity, load balancing, and partitioning to enable high availability.

Azure services have redundant components; if one experiences a hardware failure or must be temporarily taken down to upgrade its software, the service remains available through other instances. This also supports scalability because the number of redundant instances of a service can be easily adjusted according to load.

Access to all services from the Internet goes through a load balancer, which divides resource usage among the service instances that are currently operating. All customer services and most internal Azure services are provided by VMs running on a host server over a Windows hypervisor. The Fabric Controller (FC) is responsible for allocating VMs on host servers when customers request that instances be created, or whenever a new one is needed because an existing VM has failed.

Azure Storage Services are also provided using this same mechanism, with all data stored redundantly and a load balancer is responsible for dividing traffic among functioning components. Azure is deployed in globally distributed datacenters whose networks are connected via peering relationships with a large number of ISPs around the world to provide high performance access from almost anywhere. At each entry point from the Internet, Microsoft implements a shared firewall and Distributed Denial-of-Service (DDoS) mitigation system. This network is separate from Microsoft's corporate network used to support its employees in their daily activities and software development efforts.

4 Azure Security Overview

4.1 Authentication and Identity Management

Azure offers Multi-Factor Authentication (MFA) to help safeguard access to data and applications while providing a simple sign-in process. It delivers strong authentication while allowing users a wide array of verification options including phone call, text message, or mobile application notification. It also provides real-time alerts to your IT department, informing them of suspicious account credentials and inconsistent log-in patterns.

Azure MFA can be deployed on-premises, in the cloud, or in a hybrid mode, and can be used to help secure VPNs, Active Directory Federation Services, Microsoft IIS web applications, Remote Desktop, and other remote access applications using RADIUS and LDAP authentication.

Active Directory and other on-premises directories can be extended to Azure Active Directory (Azure AD) for single sign-on to all cloud-based applications and automatic synchronization of user attributes. Azure AD also offers developers an effective way to integrate identity management into their applications. Industry standard protocols such as SAML 2.0, WS-Federation, and OpenID Connect makes sign-in possible on a variety of platforms such as .NET, Java, Node.js, and PHP. Azure AD also offers a REST-based Graph API and support for OAuth 2.0.

Note that Azure MFA can be used to secure access not only to a company's digital asset workflows, but also to ensure secure and appropriate access to corporate data such as email systems, documents, and other stored data.

For more information on Azure MFA, see http://azure.microsoft.com/en-us/services/multi-factor-authentication/. To learn more about integrating your existing directory solution with Azure, see http://azure.microsoft.com/en-us/services/active-directory/.

4.2 Encryption

Azure offers customers the flexibility to implement additional encryption and to manage their own keys, both on-premises and in the cloud.

To help protect data while in transit, Azure uses industry-standard transport security protocols between user devices and Microsoft datacenters, as well as within the datacenters themselves. You can enable encryption for traffic between your own virtual machines (VMs) and end users.

When using virtual networks, you can use IPsec to encrypt traffic between your corporate VPN gateway and Azure. For data at rest, e.g. stored on a hard drive, Azure offers a wide range of encryption capabilities up to AES-256, giving you the flexibility to choose the solution that best meets your needs.

The use of encryption and related technologies to secure and enable specific media workloads is covered in section 5.3.

4.3 Managing Keys and Secrets

Secure key management is essential to protecting data in the cloud. With Azure Key Vault, there is no need to provision, configure, patch, and maintain your own key management software. Azure Key Vault streamlines the key management process and enables you to maintain control of keys that access and encrypt your data.

Key Vault is designed so that Microsoft cannot see or extract your keys. Uniquely, Key Vault lets you encrypt keys *and* small secrets such as authentication keys, storage account keys, data encryption keys, .PFX files, and passwords.

For added assurance, keys can be stored in Hardware Security Modules (HSMs), specialized, tamperproof processors that can delete keys if tampering is detected. Key Vault's HSMs are certified to FIPS 140-2 level 2 standards, ensuring that your keys stay within the HSM boundary. You can provision new vaults and keys (or import keys from your own HSMs) in minutes and centrally manage keys, secrets, and policies. You maintain control over your keys – simply grant permission for your own and third party applications to use them as needed. Applications never have direct access to keys. Developers can easily manage keys used for dev/test and migrate seamlessly to production keys managed by security operations. HSMs can also be employed to manage keys for SQL Databases (Transparent Data Encryption and Column Level Encryption).

You can improve performance and reduce latency of cloud applications by storing cryptographic keys in the cloud instead of on-premises. Key Vault rapidly scales to meet the cryptographic needs of your cloud applications and match peak demand without the cost associated with deploying dedicated HSMs.

You can achieve global redundancy by provisioning Vaults in Azure global datacenters, although it is highly recommended that you keep a copy of your encryption keys in your own HSMs for added durability. You can also create one or more vaults to hold secrets and maintain appropriate segmentation and management of secrets. It should also be noted that access controls for secrets is independent of access controls for keys.

You can monitor and audit key use with Azure logging by piping logs into HDInsight or your SIEM solution for additional analysis and threat detection.

To learn more about Azure key management, go to http://azure.microsoft.com/en-us/services/key-vault/

4.4 Network and Service Isolation

Azure prevents different customers' tenant VMs from communicating with each other by segregating them through a series of logical isolation mechanisms. The systems managing access to customer environments (the Azure Portal, SMAPI, etc.) are also isolated within an Azure cloud service operated by Microsoft. This logically separates customer access infrastructure from customer applications and storage.

4.4.1 System Isolation

The isolation of customer infrastructure on a public cloud is fundamental to maintaining security. The most basic and critical boundary preventing inter-tenant communications is the isolation of the host system from the guest VMs, and the guest VMs from one another, hosted by the hypervisor and the host OS. A combination of packet-filtering firewalls on host and guest VMs, plus comprehensive access controls on virtual networks, help maintain the integrity of tenant workloads.

VM isolation can be enforced through other mechanisms, as well. Running applications with the "least privilege" required is widely regarded as an information security best practice. Customer software should be restricted to running under a low-privilege account by default, which helps protect the customer's service from attack by its own end users.

4.4.2 Network Isolation

Azure's hypervisor and the host OS provide network packet filters that help assure VMs cannot generate spoofed traffic, cannot receive traffic not addressed to them, cannot direct traffic to protected infrastructure endpoints, and cannot send or receive inappropriate broadcast traffic. Storage nodes run only Azure-provided code and configurations, and access control is thus narrowly tailored to permit legitimate customer, application, and administrative access only. Network access to VMs is limited by packet filtering at the network edge, at load balancers, and at the host OS level.

The cumulative effect of these restrictions is that each cloud service acts as though it were on an isolated network where VMs within the cloud service can communicate with one another, identifying one another by their source IP addresses with confidence that no other parties can impersonate their peer VMs. VMs must be configured to accept incoming connections from the Internet over specific ports and protocols.

Azure supports a powerful set of additional network security capabilities, which customers are encouraged to leverage to enhance resource isolation, access control, and resilience across their implementations.

Hybrid Clouds: Azure supports Virtual Networks, which act as a trust boundary and enable VMs to function as part of a customer's internal (on-premises) network. This allows for increased security in the deployment of hybrid cloud and on-premises solutions. Azure-based VMs connected to VNETs can be domain-joined to customer domain controllers in order to be managed consistently with the customer's on-premises resources.

Isolated Private Networks: A customer may deploy multiple logically isolated private networks. These sub-divided networks can be categorized as deployment networks or virtual networks. Deployment networks enable each deployment to be isolated from the other deployments at the network level. Multiple VMs within a deployment can communicate with each other through private IP addresses. Virtual networks, on the other hand, are isolated from the other virtual networks. Multiple deployments inside the same subscription can be placed on the same virtual network, and then communicate with each other through private IP addresses.

Virtual Networks: Azure Virtual Networks offer numerous capabilities that help ensure security and compliance. Of particular note are *user defined routes*, which provide complete control over the traffic flow in your virtual network. Virtual networks by default provides system routes for traffic flow between virtual machines, but the routing tables can be customized by defining routes allowing you to direct traffic through virtual appliances such as application firewalls, gateways, NAT devices, IPS and IDS devices, etc.

More information about user defined routes can be found at http://azure.microsoft.com/en-us/documentation/articles/virtual-networks-udr-how-to, but in short, they help ensure that your content cannot be accidentally or maliciously misdirected in ways that compromise security. It should also be noted that Azure has enhanced its ability to support reserved IP addresses, enabling you to move reserved IP addresses between services and re-direct traffic from one service (set of one or more VMs) to another service. This feature is useful in scenarios where you want to reduce the impact of downtime by quickly moving IPs between VMs.

Private Network Connections: Azure also offers ExpressRoute: direct, private network connectivity to Azure that bypasses the Internet and provides better network performance, predictability, and privacy. ExpressRoute is particularly useful for those organizations that want to maintain the security and compliance of their existing WAN while leveraging the global scale of Azure to deliver truly global services through the cloud.

An ExpressRoute circuit can also be routed through Azure's VPN Gateway, allowing you to use a site-to-site VPN tunnel as a backup for your private ExpressRoute connection. This powerful coexistence of site-to-site VPN and private ExpressRoute connections helps ensure and enhance not only the security of the network but also its availability and performance. The combination of ExpressRoute and VPNs also allows you to connect branch offices that aren't part of your WAN to your Azure virtual networks, and also enables numerous mobile worker scenarios.

Network Security Groups (NSG): NSGs allow you to create security boundaries for workloads by implementing allow and deny rules. These rules can be applied at the NIC level (VM instance level) or at the subnet level (group of VMs), and different rules can allow or deny different types of traffic. Rules can be useful for directing specific traffic to specific endpoints, such as application firewalls, or together with Traffic Manager Profiles to divert traffic from unhealthy endpoints based on policies and monitoring.

Application Gateways: Application Gateways provide a mechanism for isolating public and private encrypted network traffic, much like a proxy server in a physical network. Azure Application Gateways can function as an SSL bridge that will redirect traffic after decrypting it and determining the proper destination.

4.5 Integrity Controls

The integrity of Azure is carefully managed from bootstrap through operation. The host OS that runs on physical nodes is a hardened operating system. After a compute node is booted, it starts the Fabric Agent and awaits connections, authenticating bi-directionally via TLS. Such communications are via one-way push, making it harder to attack services higher in the chain of command because they cannot make requests directly to those components.

5 Azure Media Services

Azure Media Services is an extensible, cloud-based platform that enables developers to build scalable media management and delivery applications. Media Services is based on REST APIs that enable you to more securely upload, store, encode and package video or audio content for both on-demand and live streaming delivery to various clients (for example, TV, PC, and mobile devices).

A detailed diagram depicting various Azure Media Services workflows, from media creation through consumption, can be found at http://www.microsoft.com/en-us/download/details.aspx?id=38195.

5.1 Content Distribution

Azure allows you to build new channels to distribute your digital products. The two primary workflows discussed in this paper are enabling streaming services and on-demand consumption services.

5.1.1 On Demand

Azure Media Services lets you protect content in storage and deliver streaming media in either non-encrypted or encrypted form. To set up a security-enhanced on-demand stream, first upload the digital asset into storage, using the storage encryption option to protect your content both during upload and while at rest. Then, encode it with adaptive bitrate MP4. Once packaged, publish the asset by creating an OnDemand locator. (Note: It is important that you configure at least one streaming reserved unit on the streaming endpoint from which you want to stream content.)

More information on the this workflow and controls can be found at http://azure.microsoft.com/en-us/documentation/articles/media-services-video-on-demand-workflow/

Publish encrypted content by uploading the asset, encrypting the storage unit, and encoding the content. At this point in the process, you must then create an encryption content key for the asset you want to be dynamically encrypted during playback, and configure the content key authorization policy. For more information of managing keys, see Managing Keys and Secrets above.

Once this is completed, the asset can be published as before.

5.1.2 Streaming

Azure Media Services lets you create streaming services that can:

1. Ingest live content using various live streaming protocols (for example RTMP or Smooth Streaming)
2. Encode your stream into an adaptive bitrate stream
3. Preview your live stream
4. Store the ingested content in order to be streamed later (Video-on-Demand)
5. Deliver the content through common streaming protocols (for example, MPEG DASH, Smooth, HLS, HDS) directly to your customers, or to a Content Delivery Network (CDN) for further distribution.

In most cases, the content being streamed will be pre-recorded (e.g. a movie), but live content (e.g. a sporting event) can also be streamed with Azure.

For the best customer experience, you need to be able to deliver high quality video to various devices under different network conditions. To effectively manage quality, encode your content to a multi-bitrate (adaptive bitrate) video stream. When streaming on different devices, use Media Services dynamic packaging to dynamically re-package your stream to different protocols. Media Services supports delivery of the following adaptive bitrate streaming technologies: HTTP Live Streaming (HLS), Smooth Streaming, MPEG DASH, and HDS (for Adobe PrimeTime/Access licensees only).

Azure Media Services Channels, Programs, and Streaming Endpoints handle all live streaming functionality including ingest, formatting, DVR, security, scalability and redundancy.

For more detail on configuring a live streaming service, see http://azure.microsoft.com/en-us/documentation/articles/media-services-live-streaming-workflow/.

5.2 Consumption

In addition to supplying the technologies necessary for creating security-enhanced distribution channels for digital assets, Azure Media Services also provides the tools needed to create rich, dynamic client player applications for most platforms, including Web browsers, iOS, Android, Windows devices, Xbox, and set-top boxes.

Azure Media Player is a web video player designed to play back media content from Microsoft Azure Media Services on a wide variety of browsers and devices. Azure Media Player utilizes industry standards such as HTML5, Media Source Extensions (MSE), and Encrypted Media Extensions (EME) to provide an enriched adaptive streaming experience. Coupled with a unified JavaScript interface to access APIs, this ensures that content served by Azure Media Services can be played across a wide-range of devices and browsers without any extra effort.

To ensure asset security as defined in CDSA/CPS Capability 5.10.8 *Encryption* and 5.22 *File Transfer Management*, Azure Media Services allows for dynamic encryption of assets with PlayReady encryption or AES-128-bit envelope encryption.

As mentioned previously, we recommended that you deploy at least one streaming unit for the streaming endpoint from which you plan to deliver your content; this is particular necessary to play dynamically packaged or dynamically encrypted content. This can be done through the Azure Management Portal, which also provides a content player that you can use to test your assets prior to distribution. Note that this configuration also helps address the requirements of CDSA/CPS Capabilities 3.4 *Asset Handing and Transfer* and 7.1 *Business Continuity*.

5.3 Content Protection

Azure provides several mechanisms to help protect digital content while at rest and in transit, as well as tools to restrict the use of said content to only authorized users and/or customers.

5.3.1 Encoding Services

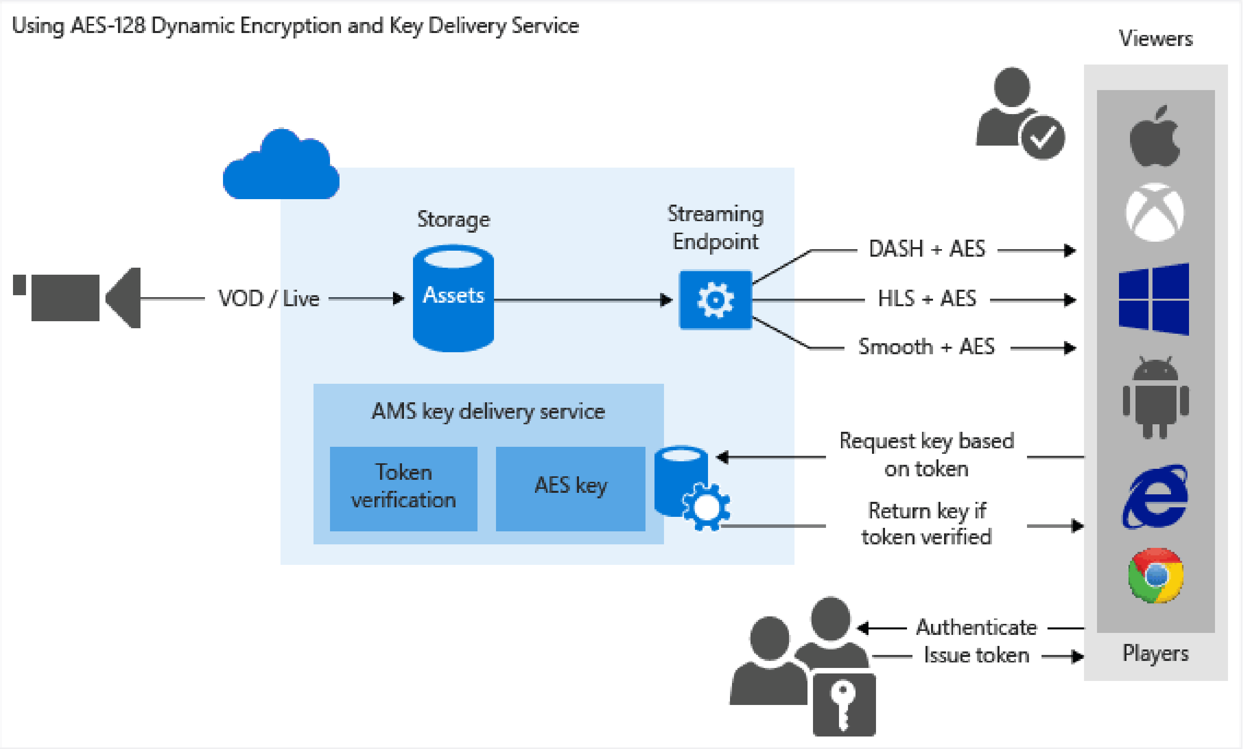
An on-premises live encoder sends multi-bitrate RTMP or Smooth Streaming (Fragmented MP4) to your Azure Channel. You can use live encoders that output multi-bitrate Smooth Streaming, including Elemental, Envivio, and Cisco. The following live encoders output RTMP: Adobe Flash Live, Telestream Wirecast, and Tricaster transcoders. The ingested streams pass through Channels without any further processing. Your live encoder can also send a single bitrate stream, although this is not recommended when trying to maintain consistent streaming quality.

5.3.2 Dynamic Encryption

In Azure Media Services, there are two ways to encrypt your content, regardless of whether you are applying common encryption (PlayReady) or envelope encryption (AES): dynamic or static. For flexibility of delivery, it is recommended that you use Azure's dynamic encryption capabilities.

Once you encode your file into multi-bitrate MP4, you can configure the file to be encrypted by defining the Content Key, Content Key authorization policy, and asset delivery policy. The file is stored in clear text by default, so it is advisable to place storage encryption on the container (which is optional). After configuration, the Azure streaming server will apply sample level encryption on your media file on-the-fly.

For example, if you configure AES dynamic encryption for HLS streaming protocol, Azure will encrypt your file on-the-fly with AES envelope encryption and deliver through HLS. Below is a diagram to show you how dynamic encryption works in Azure Media Services:



Dynamic encryption helps you save on storage costs, as you only need to save your media file once, and encrypt it differently as needed. Alternatively, if you pre-encrypt the file and want to change the content key, you will need to re-encrypt it, which could be time-consuming and costly.

In addition, dynamic encryption lets you change your key at any time, and the streaming server will automatically pick up the new key for content delivery. Moreover, if you want to change your content into clear format in the future, you just need to remove the encryption configuration and the file will be served in the clear.

For those who prefer to statically encrypt their files, Azure's Static Encryption feature allows you to encrypt your content with either an AES 128-bit key or PlayReady license, and the encrypted file will be stored as-is. Azure's streaming server will deliver the encrypted bits when your player requests. If you wish to use static encryption with Azure Media Services, the input file format has to be Smooth Streaming. Static encryption is most appropriate when your files have already been encrypted on-premises and you plan to only deliver the file through one specific protocol.

5.3.3 Digital Rights Management (DRM)

As noted above, Azure Media Services enable you to secure your media from the time it leaves your computer through storage, processing, and delivery with dynamic encryption and PlayReady DRM.

Azure Media Services also provides a service for delivering PlayReady licenses and AES clear keys to authorized clients. You can use the Azure Management Portal, REST API, or Media Services SDK for .NET to configure authorization and authentication policies for your licenses and keys.

When the end-user player tries to play your PlayReady-protected content, a request is sent to the license delivery service to obtain a valid license. If the service approves the request, it issues the license which is then sent to the client and can be used to decrypt and play the specified content. Licenses contain the rights and restrictions that you want the PlayReady DRM runtime to enforce when a user plays back protected content. Media Services provides APIs that let you configure your PlayReady licenses.

5.3.4 Encrypted Storage

Another option for protecting media assets in Azure Storage is to encrypt it on-premises with AES-256 and then upload it using the *StorageEncrypted* option. This helps protect your content at rest when being used as input to the Media Processor pipeline, including encoding and packaging tasks. Assets protected with *StorageEncrypted* are automatically decrypted and placed in an encrypted file system prior to encoding. You can specify whether the assets that are created as a result of encoding or packaging tasks be storage-encrypted, as well.

In order to deliver a storage encrypted asset, you must use dynamic encryption and configure the asset’s delivery policy (IAssetDeliveryPolicy) so that Azure Media Services knows how you want to deliver your content. Before your asset can be streamed, the streaming server removes the storage encryption, and then streams it using the specified delivery policy.

For example, to deliver your asset encrypted with AES, set the policy type to DynamicEnvelopeEncryption. To remove storage encryption and stream the asset in the clear, set the policy type to NoDynamicEncryption. For other delivery policy types, see AssetDeliveryPolicyType.

6 Service Operations

The CDSA/CPS standard is as much about the processes and controls for managing your infrastructure as it is about particular technologies. Among these considerations are process documentation, change and asset management, personnel policies, and training. In addition, CDSA addresses corporate governance issues such as business continuity and disaster recovery planning. These issues are specifically covered in CPS Capability Frameworks 1, 2, 3, 6, and 7.

6.1 Policies and Procedures

The Azure governance framework consists of Microsoft corporate and Azure policies, standard operating procedures and standards that together form a comprehensive and detailed control structure. The Microsoft corporate security policy, Azure Information Security Management System (ISMS), and Azure Information Security Policy form the overarching governance documents. Local legal teams ensure that territorial legislative requirements are reflected in governance applicable to that area.

6.2 Security and Risk Management

Azure risk management is guided by standard operating procedures designed to ensure compliance with NIST 800-37 and similarly rigorous guidelines. The assessment process is managed by the compliance team and identifies threats, safeguards and vulnerabilities before assessing risk through an impact/likelihood matrix.

The risk register is built upon the NIST Threat List using a range of internal resources. Risk management outputs are reviewed at both the Azure and Microsoft corporate level. Security incident management practices are also guided by standard operating procedures designed to ensure an effective response to incidents by following a five stage process from incident detection through root cause analysis.

A detailed description of Azure incident management and operations can be found at http://www.microsoft.com/security/msrc/default.aspx.

6.3 Personnel and Training

Microsoft Azure developers and cloud administrators have been given only the level of privileges that they need to carry out their assigned duties to operate and evolve the service. As noted throughout this document, Microsoft deploys combinations of preventive, detective and reactive controls to help protect against unauthorized developer and/or administrative activity, including:

- Tight access controls on sensitive data, including a requirement for two-factor smartcard-based authentication to perform sensitive operations
- Combinations of controls that greatly enhance independent detection of malicious activity
- Multiple levels of monitoring, logging, and reporting

Microsoft operations personnel follow a formal process when they are required to access a customer's subscription or related information, and this is only done at the customer's request or in response to security incidents where there is evidence of misbehavior on the part of the customer's software.

For more information about these and other operational controls, Microsoft recommends that customers review the Azure Trust Center at http://azure.microsoft.com/en-us/support/trust-center/compliance/.

Confidentiality agreements with employees and vendors are part of staff and third party contracts. Mandatory security training is delivered to new and existing employees and third parties annually.

6.4 Asset Management

Asset management is governed by a number of Microsoft corporate and Azure policies, and is specified in CPS Framework 3, *Asset Management*. The technical nature of Azure services mean that customers remain responsible for significant parts of the data asset operation chain. Customer data may be transferred to and from the Azure environment digitally or on physical hard drives and both processes are subject to stringent security controls. Azure encrypts customer data whilst in transit and recommends and supports encryption of data at rest.

When a system reaches the end of its life, Microsoft operational personnel follow rigorous data handling procedures and hardware disposal processes to assure that no hardware or media that may contain customer data is made available to untrusted parties.

6.5 Datacenter Operations

The Azure network is a highly sophisticated physical and virtual environment working across a global network of datacenters. Azure datacenters are constructed to a common design with layered security controls incorporated into the build. Regional Security Operations Managers provide oversight of datacenter security 24/7/365. Physical access is restricted using technical controls at local levels with global oversight through the Datacenter Access Tool, and is supported by uniformed guards.

Security is embedded at all levels through sophisticated technical controls, monitoring and logging and standard operating procedures. IT system access is strictly controlled following the principle of least privilege and procedures are in place to manage staff changes. The network is closely monitored for security incidents and resources are available 24/7 to respond if required. Security patching and anti-virus measures are in place and applied to the physical network and virtual machines.

6.6 Redundancy and Business Continuity

Business continuity is a key deliverable of Azure, which offers customers different levels of data resilience. All customer data is duplicated threefold either within a single datacenter, across a region or globally. Azure datacenter infrastructure has a high degree of redundancy built in at all levels including network device duplication, meshed connectivity and long term, full load backup power capability. Specifically, Azure runs in geographically distributed Microsoft facilities, sharing space and utilities with other Microsoft Online Services.

Each facility is designed to run 24/7/365 and has a minimum of two sources of electrical power, including a power generation capability for extended off-grid operation. Environmental controls are self-contained and remain operational as long as the facility and contained systems remain online. These datacenters comply with a myriad of industry standards (such as ISO 27001) for physical security and availability and are managed, monitored, and administered by Microsoft operations personnel.

7 References and Further Reading

The following resources are available to provide more general information about Microsoft Azure and related Microsoft services, as well as specific items referenced in the main text:

- Microsoft Azure Home – general information and links about Microsoft Azure
  - http://www.microsoft.com/windowsazure/
- Microsoft Azure Developer Center – developer guidance and information
  - http://msdn.microsoft.com/en-us/windowsazure/default.aspx
- Security Best Practices For Developing Microsoft Azure Applications (white paper)
  - http://download.microsoft.com/download/7/3/E/73E4EE93-559F-4D0F-A6FC-7FEC5F1542D1/SecurityBestPracticesWindowsAzureApps.docx
- Crypto Services and Data Security in Microsoft Azure (article)
  - http://msdn.microsoft.com/en-us/magazine/ee291586.aspx
- Microsoft's Security Development Lifecycle (SDL)
  - http://www.microsoft.com/security/sdl/
- Microsoft Cloud Infrastructure and Operations group
  - http://www.microsoft.com/en-us/server-cloud/cloud-os/global-datacenters.aspx
- Microsoft MCIO ISO 27001 certification
  - http://www.bsigroup.com/en-US/Our-services/Management-system-certification/Certificate-and-Client-Directory-Search/Certificate-Client-Directory-Search-Results/?searchkey=company%3dMicrosoft%2b&licencenumber=IS 587621
- Microsoft Security Response Center [where Microsoft security vulnerabilities, including issues with Microsoft Azure, can be reported]
  - http://www.microsoft.com/security/msrc/default.aspx
  - Or via email to secure@microsoft.com.
- Content Delivery and Storage Association (CDSA) Content Protection and Security (CPS) Standard
  - http://www.cdsaonline.org/wp-content/uploads/2010/06/CPS-Standard-March-2014.pdf