◄SNOCAP►

SNOCAP MyStore

Embeddable Commerce Infrastructure

Introduction

SNOCAP MyStore is a system allowing artists and organizations who own rights to digital content to create interactive storefronts that can be embedded into web pages. These storefronts not only let consumers preview, purchase and download digital music, they can be easily copied by the consumer to other web pages. Additionally, all user interactions necessary to fulfill commerce transactions are conducted directly in the storefront—the consumer is not redirected to another web page. This document provides an overview of the SNOCAP MyStore product, the capabilities it provides artists and consumers, and the components that make up the system.

MyStore Capabilities

MyStore allows independent artists and music labels to:

- upload and register their musical works and information that describes it

- specify wholesale pricing on a per-track basis

- generate a web-based storefront that they can embed in any web page they wish
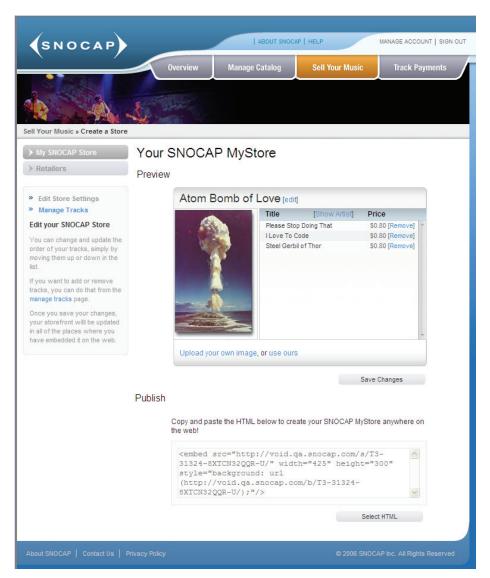
- collect revenue generated from sales

Web sites hosting MyStore storefronts benefit by:

- providing users access to popular and unique content

- encouraging the viral exchange of artist's stores, strengthening the social network community

- avoiding the cost of screening uploaded content for fraud, hosting the content, and fulfilling downloads

For consumers, MyStore provides:

- a convenient way to purchase and download music they can't find on other paid services, and in a format that works with their favorite music player

- a trusted mechanism to pay for their purchases, with a single user account across all stores

- an easy way to support their favorite artists

MyStore makes use of the SNOCAP Rights Management Service (RMS) and its ability to authorize, record, and fulfill the purchase and download of tracks registered with SNOCAP. Artists use the SNOCAP Registry web application to upload their tracks, apply license information, and specify which tracks are to be presented in the MyStore consumer-facing storefront. Other parameters affecting the MyStore storefront, including the name and image displayed in the user interface, are also configured in the SNOCAP Registry.

As part of the MyStore setup, artists are provided with an HTML snippet they can embed in any web page they wish to contain a storefront. This HTML refers to an Adobe Flash® object that implements the store user interface. The Flash-based MyStore storefront allows consumers to view the available tracks and prices, listen to 30 second clips, purchase tracks, and download the audio files to their computers.

When accessed, the MyStore storefront retrieves data specific to the store instance being displayed. This information is used to render the tracks for sale, the name of the store, the store image, and the prices associated with each track. User interaction with the storefront is either processed locally in the
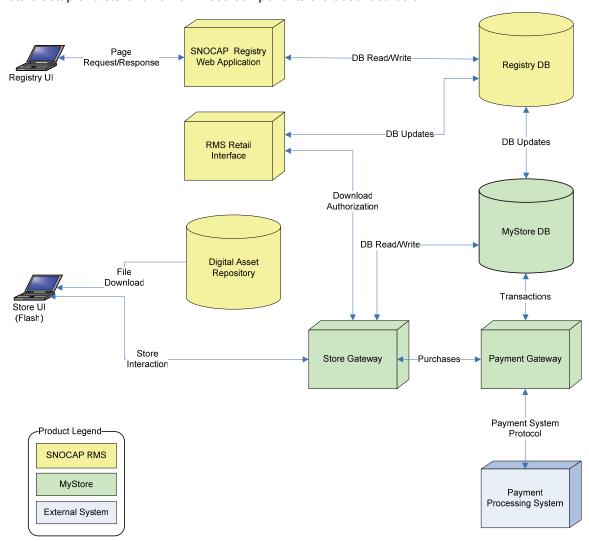
Copyright © 2006 SNOCAP, Inc.

browser, or causes a request to be made to the back-end systems that provide the MyStore services. MyStore back-end systems process requests to authenticate the user, access their accounts, and deliver purchased audio files.

System Overview

The MyStore architecture is designed to accommodate a large number of store instances embedded in many web pages, and a high volume of purchase and download transactions. Proven techniques are used to implement scalability and failover, and industry-standard security best practices are employed throughout the system.

System Components

MyStore is implemented as a system of loosely coupled components that work together during store setup and store run time. These components are described below.

Registry User Interface

This is the browser-based interface presented to the artist to register tracks, apply license terms, and configure the parameters that affect the store.

Registry Web Application

This represents the components that generate pages presented in the Registry user interface and enforce the behavior and business rules of the RMS. This code invokes database APIs to set and get values stored in the Registry database.

Registry Database

This is the core database for the SNOCAP Rights Management Service containing all data about tracks, licenses, organizations—everything that is presented in the Registry web application, and used to support the RMS functionality.

MyStore Database

This is the database used by MyStore. It receives track and license information updates from the Registry database and sends transaction records to the RMS for accounting purposes. It contains information, including retail pricing and consumer account information, necessary for the MyStore application.

Store User Interface

The consumer-facing user interface that represents a storefront is implemented as a Flash application. This application interacts with the Store Gateway to obtain data specific to the store instance (the track list and prices, store name, and store image) and to conduct purchase transactions. The Store UI prompts the consumer for account information when the initial purchase action is taken, collecting the data necessary to establish a MyStore account and associate it with a PayPal account. The account credentials are used by the Store Gateway to debit the consumer's account when purchases are made.

Store Gateway

This is a server component that provides a secure API used by the MyStore storefront to conduct back-end operations. It communicates with the SNOCAP RMS to authorize downloads and record purchases. It also communicates with the Payment Gateway to debit a consumer's account for the amount of the transaction. The Store Gateway also interfaces with the MyStore database to get track information and prices, authorize users, and record payment transactions. The Store Gateway is invoked by the external Payment System when transactions occur and records this information in the MyStore database.

RMS Retail Interface

This represents the real time interface between the SNOCAP RMS and the MyStore application. It authorizes and records downloads and provides access to digital assets in the Digital Asset Repository.

Payment Gateway

This component provides an interface between an external payment system and the Store Gateway. Communication with the external systems is done via a web services API. MyStore uses PayPal as the payment system, although integration with other providers is easily accommodated by this design.

Digital Asset Repository

This is the repository containing audio files available for download by retail applications. It provides security so that unauthorized file downloads are not possible. To achieve the level of scalability and availability required for MyStore, industry-standard edge-caching services are used between the Digital Asset Repository and the consumer.

Scalability Considerations

MyStore performance requirements encompass several dimensions:

- Accommodate high load on the Registry web application

- Accommodate a large number of MyStore consumer application instances

- Concurrently conduct a large number of purchases

- Concurrently deliver a large number of audio files

Each of these areas is discussed below.

Web Application Load

The systems implementing the Registry web application scale linearly using standard web server clustering techniques. Extra machines are added if excessive load is reached. Performance is measured on these servers by monitoring the average response over a rolling time window. When a predefined threshold is hit, SNOCAP operations staff are notified and additional servers are deployed. SNOCAP maintains a pool of reserve servers for this purpose.

MyStore Consumer Application Load

The consumer-facing store is a Flash application (shockwave file) served from the web server infrastructure used to support the Registry web application, and cached using industry-standard edge-caching services. When a MyStore storefront loads, it reads the track information to be displayed from the Store Gateway. The Store Gateway caches this information so that the MyStore database is not accessed. Extra Store Gateway machines are added if excessive load is reached. Performance is measured on these servers by monitoring the average response of store loading operations over a rolling time window. When a predefined threshold is hit, SNOCAP operations staff are notified and additional servers are deployed. SNOCAP maintains a pool of reserve servers for this purpose.

Purchase Processing Load

Purchase processing consists of

1. Preauthorizing the track download given parameters indicating the track and license terms being executed

2. Invoking the external purchase system to debit the consumer's account

3. Using this payment information to authorize the file download

The SNOCAP RMS retail interfaces provide the link to the MyStore system to perform the first and third of these steps. The systems supporting the RMS retail interfaces are clustered, and their load can be linearly scaled by the addition of retail interface servers to the RMS.

The second step in purchase processing involves the Store and Payment Gateways. These servers are also clustered, and work is distributed to them using standard load balancing techniques. For the gateway servers, performance is measured by monitoring the average response over a rolling time window. When a predefined threshold is hit, SNOCAP operations staff are notified and additional servers are deployed. SNOCAP maintains a pool of reserve servers for this purpose.

Audio File Download Processing Load

Audio files are served from the SNOCAP Digital Asset Repository and are cached using industry standard edge-caching services. This approach satisfies high load requirements by offloading content delivery to the edge caching platform, which provides optimal performance, 100% uptime, and tremendous scalability. The caching system uses the DNS-based network intelligence mechanism to direct end users to the cache for all requests for objects from the Digital Asset

Repository, pulling content from the Repository only when it has not yet been cached or an updated version of the asset is available.

Security Considerations

MyStore security considerations encompass the following:

- Fraudulent access to the Registry web application

- Fraudulent registration of audio content

- Unauthorized access to consumer account information

- Unauthorized access to audio content

- Physical security of the facilities housing SNOCAP computing systems

These considerations are discussed below.

Web Application Security

Access to the SNOCAP Registry web application requires user-supplied credentials, which must be greater than a defined minimum length and require periodic updates. Accounts in the SNOCAP system require registration and approval prior to their creation. Third-party identity verification services are used to validate information about the user. If insufficient verification data is obtained, a SNOCAP customer care representative reviews the application.

Content Registration Security

User accounts are tiered based on the type of organization with which the account is associated. Individual content providers have limited capabilities in the system relative to larger organizations (for example, independent and major record labels), and content they register must correspond to the artist names they represent at account creation time. Furthermore, audio content that is uploaded into the SNOCAP system is identified using the SNOCAP Content Identification System. This system identifies audio content based on its acoustic data, and therefore is not susceptible to misidentification due to erroneous metadata or changes to file format, filename or bit rate. The fingerprinting infrastructure maintains a database of fingerprints which is updated as new content is received. This system allows for the detection of content registered by multiple parties, and flags such instances for resolution based on a variety of business rules that consider the type of organizations making the claim and the order in which the claims were made.

Consumer Account Security

SNOCAP uses PayPal's PreApproved Payments product to charge MyStore consumers for purchases. In order to make a purchase, a consumer must verify their PayPal account and establish a billing agreement through PayPal that grants SNOCAP permission to bill the customer at will, up to a negotiated maximum payment amount per month. SNOCAP never has direct access to PayPal's member account information. Along with the MyStore username and password, SNOCAP securely stores the consumer's unique PayPal Payer ID, email address, and Billing Agreement ID returned by PayPal. This information is sent to SNOCAP by PayPal over a secure connection once a customer has verified their account and established the billing agreement. The customer can cancel the billing agreement with SNOCAP at any time through their PayPal account. To change their account information, the consumer logs in to their PayPal account—SNOCAP is completely removed from this process.

The security of PayPal member's information, transactions, and money is the core of their business and their top priority at PayPal. PayPal automatically encrypts member's confidential information in transit from the member computer to PayPal's using the Secure Sockets Layer protocol (SSL) with an encryption key length of 128-bits (the highest level commercially available). Before members even register or log in to PayPal, their server checks that the member is using an approved browser - one that uses SSL 3.0 or higher. Once the member information

reaches PayPal, it resides on a server that is heavily guarded both physically and electronically. PayPal's servers sit behind an electronic firewall and are not directly connected to the internet, so all member's private information is available only to authorized computers.

Audio Content Access Security

SNOCAP protects against unauthorized access of audio content by using security capabilities offered by industry leading edge-caching services. SNOCAP uses a centralized authorization mechanism, passing data used to authorize the request in the query string. The query string used by the Store Gateway and delivered to the MyStore storefront as part of the download URL contains signed information that, with a secret key shared between the Store Gateway and the SNOCAP RMS, is used to validate that the information sent in the request is valid. If so, the RMS authorizes the edge caching system to deliver the audio file.

Physical Security

SNOCAP maintains a high degree of security in our facilities, systems and processes to ensure that the content and services we provide are protected from unauthorized access and tampering.

System Location

SNOCAP's production environment is located in a SAS 70 certified co-location facility. The facility is monitored 24x7 by co-location facility personnel using CCTV systems. Network and system monitoring is done by SNOCAP.

Protection Against Unauthorized Local Access

Access to the co-location facility is limited to personnel on an authorized access list maintained by our co-location facility and SNOCAP's Director of Operations. SNOCAP's production environment is located within a locked cage. SNOCAP will limit direct hardware access to the production environment to SNOCAP's Director of Operations, Database Administration staff and SNOCAP IT staff. In addition, physical hardware access may be granted at the discretion of SNOCAP's Director of Operations to maintain racks, power systems, cabling and contain physical damage. All access to machines is logged over the network to a secure logging server.

Protection Against Unauthorized Network Access

SNOCAP's production environment is segmented into multiple VLANs to limit potential security breaches. The systems are behind a firewall that prevents direct access from the Internet except for public network services. Each machine has a small number of authorized user accounts. Machines are accessed using SSH only. All access to machines is logged over the network to a secure logging server.