Understanding Your Enterprise API Requirements

Part 1 – The 5 Phases of API Management

Deliver web and mobile-enabled APIs to develop new revenue channels, build rich interaction with prospects, and collaborate more efficiently with partners.

Applications – it's a whole new world

Social media, mobile and cloud computing have changed the way we interact with applications. For users, what was once a one-pronged experience, with a single interface or point of interaction, is now a collection of interactions between applications and functions. This combination, called a mashup, delivers new, more complex and more useful capabilities to users on their devices.

For example, the Starbucks' iPhone application uses Google Maps to locate nearby Starbucks coffeehouses, communicates with Starbucks' point-of-sales system to place orders, and transacts with Blackhawk Network to buy and refill Starbucks gift cards. Retailers across the web embed catalogs and shopping carts within various third-party websites and mobile applications to capture impulse purchases. And online retailers offer a broad range of payment methods at checkout, integrating with credit, debit and gift card companies, reward programs and electronic wallet providers.

As the examples above demonstrate, most applications now have several interfaces, built on different technologies, targeting particular types of users, and built by a range of interested parties. Enabling these multiple interfaces to communicate, the application programming interface (API) has become the primary customer interface used for technology-driven products and services.

It's all about strategy

Enterprises can use APIs in myriad ways, and not just for retail applications. In fact, a well-executed API strategy can help any enterprise create more selling channels, better engage with customers and prospects, and offer greater value to partners. Conversely, a poor strategy delivers no value, and wastes both time and money.

axway
business. in motion.

Consumer APIs transmit information designed for public consumption, or initiate transactions that are open to the public.

Enterprise APIs transmit sensitive information or execute business transactions that are only made available to approved and authenticated counterparties.

APIs have become essential for technology-driven business, signaling a crossover from a standard to a more customer-centric, collaborative business model. The immediate success of this business model, and the potential for organizations to drive more business value through the effective delivery of APIs has created a thriving "API economy."

API management

API management – which spans publishing and promoting APIs, implementing security and usage policies, controlling access and lifecycle management, and more – is exploding as both an IT and a business discipline. The first API management showcase deployments were centered on social media, news, entertainment, basic services and consumer-oriented ecommerce APIs. As a result, common API management practice today is focused primarily on developer-enablement portals, which provide self-service for open communities of developers consuming public-facing APIs.

However, as API management becomes more popular, organizations are looking to deliver more sophisticated and complex enterprise-class APIs that transmit sensitive information or execute business transactions. The secured and scalable delivery of enterprise-class APIs requires advanced security, integration, and runtime middleware. And building an enterprise-class API management platform involves introducing new technology to existing business application infrastructure.

This white paper explains the different types of APIs and examines the five phases of API management. It is meant for enterprise architects (or others with similar responsibilities) seeking to understand the API management technology landscape, and involved in the development of API management strategy and reference architecture.

Know your APIs

Consumer vs. enterprise APIs

To build the most effective API management strategy and technology roadmap for your organization, you must start by asking what types of APIs will be delivered on your API management platform. There are two types of APIs that fundamentally drive API management requirements: consumer APIs and enterprise APIs.

Consumer APIs

Consumer APIs transmit information designed for public consumption, or initiate transactions that are open to the public. In some cases access to this information may require user authorization, which can be easily obtained from the end user because he/she owns the information.

Examples of consumer APIs and their functions include:

- Social media APIs
  - Twitter posts and Google+ profiles
  - Facebook status updates and LinkedIn contact searches
- Basic services
  - Google Maps and Bing searches
  - URL shortening services and RSS readers
- Media APIs
  - Pull New York Times headlines and Financial Times articles
  - Watch YouTube videos and look at Flickr pictures
- Information services
  - Look up weather and traffic conditions
  - View movie times and stock quotes
- Consumer ecommerce
  - Pull product catalog data and restaurant reviews
  - Add items to Amazon's shopping cart or book a reservation at Open Table

API functionality can range from consumer APIs for activities like posting on Twitter and watching videos on YouTube, to enterprise APIs for managing bank accounts or pulling patient healthcare records.

Typically, consumer APIs:

- Transmit publicly accessible information, whether for-profit or as a public service
- Transmit information owned by the end user that is not sensitive in nature
- Transmit information that is not subject to compliance and regulatory oversight
- Deliver content and services used to generate advertising revenue
- Initiate, but do not close consumer e-commerce transactions
- Provide commodity services with low switching costs

The nature of consumer APIs dictates an API management strategy that:

- Drives broad adoption to build new revenue channels
- Focuses on self-service and ease-of-adoption for low switching costs
- Does not require consumer identity validation or information integrity
- Requires minimal security, privacy, and compliance
- Requires minimal integration with existing systems

Enterprise APIs

Enterprise APIs transmit sensitive information or execute business transactions that can only be made available to approved and authenticated counterparties. Inappropriate use of enterprise APIs can result in non-trivial financial loss, legal and civil liabilities, compliance breaches, or other adverse material impact to the organization. Examples of enterprise APIs and their functions include:

When designing your API delivery strategy, note that enterprise APIs demand a higher level of operational requirements than consumer APIs.

- Financial services APIs
  - Manage personal or corporate bank accounts
  - Execute financial transactions such as wire transfers and settlements
- Healthcare APIs
  - Transmit laboratory test results
  - Access patient healthcare records
- Human resources APIs
  - Request background checks
  - Manage 401k accounts
- Supply chain APIs
  - Submit requests for quotes (RFQs)
  - Submit customs and trade documents
- E-commerce APIs
  - Place corporate purchase orders
  - Register new suppliers

Typically, enterprise APIs:

- Transmit information accessible only to approved and verified entities
- Handle business transactions that have financial impact
- Transmit information that is subject to legal or compliance requirements
- Provide services with contract-binding performance requirements
- Transmit information with national security or public safety implications

When designing your API delivery strategy, note that enterprise APIs demand a higher level of operational requirements than consumer APIs. For enterprise APIs you must:

- Enforce access control and onboarding process requirements
- Provide assurance for confidentiality, integrity, and security
- Control and provide evidence of API performance
- Provide an evidential audit trail
- Integrate with internal and business partner systems
- Comply with internal policies and compliance mandates

API sources

Your API management strategy is dependent on where your APIs are coming from. Possible sources include:

New APIs. Newly developed consumer APIs that are compatible with the latest design patterns and standards such as REST, JSON, OAuth and HTML 5.0 web sockets. Most consumer APIs tend to be new because the technology (social, mobile, etc.) is new, or the underlying technology platform has been updated to suit business needs. New APIs still require operational support from the API delivery platform such as security and monitoring.

Existing Services and APIs. Most organizations that have invested in B2B integration or Service Oriented Architecture (SOA) have an abundance of web services and APIs already in use for both internal and external point-to-point integrations. These services are usually based on standards such as SOAP, XML, EDI, or JMS. To become compatible with the new web and mobile API design patterns and standards mentioned above, these services will require a rewrite or transformation. And because existing services and APIs are used for internal or trusted B2B integrations, they will likely require extensive operational support from your API management platform to add security, control, and monitoring. Web services are typically transaction-centric (e.g. create order method), whereas web APIs are typically object-centric leveraging standard HTTP verbs (e.g. Purchase Order GET). SOAP-to-REST transformation may require advanced transformation capabilities.

Service Provider APIs
Some APIs may be built substantially on APIs provided by your vendors/service providers. Depending on the business scenario, your API management platform may need to route, aggregate, or transform service provider APIs to ensure optimal experience for your API consumers. Proper API management will also help to decouple inbound APIs from outbound APIs to preserve operational flexibility and business agility. In addition, sensitive or private information that is not to be shared with service providers must be removed, redacted, or encrypted before being sent to service provider APIs.

APIs can be new, existing, or service provider APIs. Your API management strategy is dependent on where the APIs originated, and will require security and monitoring, and possibly transformation, data extraction and encryption, and more.

The API lifecycle
The 5 phases of API management

API management is the next evolution of Service-Oriented Architecture (SOA), but it extends beyond the enterprise with web-centric architecture. Thus it should be no surprise that the API lifecycle is similar to the SOA lifecycle.

Figure 1 shows the 5 phases of API management and the technologies required at each stage to build a comprehensive API management platform. The two columns indicate the Axway technologies and third-party technologies with which Axway integrates. While consumer and enterprise APIs share the same API management lifecycle phases, they require that different emphasis be placed on the use of technology at each phase of the lifecycle. This is explained in detail in the 5 phases, below.

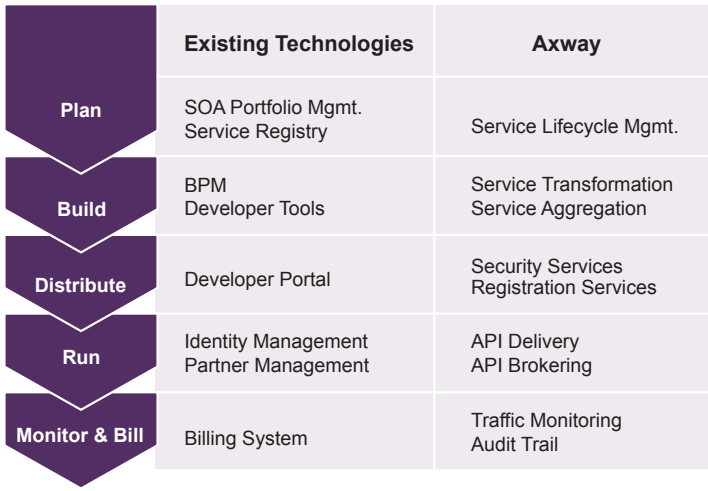

Figure 1: API lifecycle and associated technologies

Phase 1: Plan

The planning phase ensures that the right APIs are built, the right way. This involves portfolio planning, API modeling, business justification, and other aspects common to traditional SOA governance practice.

For **consumer APIs**, the planning phase is not as critical as it is for enterprise APIs. Most consumer APIs are market driven, so distribution and agility are more important than reuse and scalability. Also, for consumer APIs it's more important to be able to "experiment quickly and fail cheaply." Thus, business planning is more important than IT planning.

Enterprise APIs require more planning since they are tied to back-end transaction systems that are highly protected or secured. These APIs carry financial and business liabilities, must be carefully planned, and must remain as functionally stable as possible over long periods of time. Much of the traditional SOA planning disciplines and technologies apply directly to enterprise APIs with minimal changes.

Phase 2: Build

The build phase involves the coding and/or re-configuration of APIs. This can include developing new APIs from scratch using integrated development environments (IDE) or any variety of development tools and framework. It can also include creating new APIs by transforming existing APIs using tools and technologies such as an API Gateway, Business Process Management, or Enterprise Service Bus.

Since **consumer APIs** are mostly used with newer technology platforms, the build phase is already done as part of backend application development. For these "ready-to-use" consumer APIs, the API management platform often only has to do simple renaming or proxying of the backend APIs.

Enterprise APIs are more complicated. Most enterprise APIs are REST- or SOAP-based API frontends to legacy backend services and applications. These backend interfaces may have existed for a long time and most likely use technologies such as SOAP, SML, JMS, PL\SQL, FTP, or straight TCP. The building phase for enterprise APIs can involve complete rebuilding of new REST- or SOAP-style APIs, or utilizing a mediation technology such as a gateway to transform old interfaces.

For both consumer and enterprise APIs, if the API requires abstraction, aggregation, or mashup of third-party APIs from public-service providers (e.g. Google Maps) or partners (e.g. third-party logistics providers), then additional API brokering capabilities will be required. API brokering is the process of transforming general-purpose APIs from service providers into new APIs that are easier to consume by adding transformations that are specific to the business. API brokering requires some of the same protocol and security mediation capabilities mentioned above.

API brokering is the process of transforming general-purpose APIs from service providers into new APIs that are easier to consume by adding transformations that are specific to the business.

Phase 3: Distribute

The distribution phase involves making APIs available and driving adoption via a targeted API consumer base.

This is a very important phase for **consumer APIs** since their capacity for revenue generation is directly related to their level of adoption. For a consumer API to succeed, it is important that the API is:

- Easy for interested developers to find
- Easy to learn to use
- Supported by both the API provider and peer developers

The API technology must also be self-service so potential developers can get access to resources and get started anytime, anywhere. Since consumer APIs are usually commodity services, the switching cost is extremely low. Therefore, the API provider offering the easiest adoption experience for developers will have an advantage over its competitors. For example, if Google Maps makes it too difficult to adopt, developers will simply switch over to Bing Maps.

Enterprise APIs are very different from consumer APIs when it comes to distribution. Typically, enterprise APIs are only available to trusted business partners and the developer portal is often closed to public access. For example, companies like American Express or HSBC cannot allow public access to their enterprise APIs that transmit sensitive financial data and execute financial transactions. To gain access to enterprise APIs, partners are usually required to sign a contract, negotiate a service level agreement (SLA), or complete a security audit.

If enterprise APIs will be exposed to the general public to generate partnership interest, API traffic from unapproved applications must be routed and confined to a sandbox environment for isolation, with demonstration data only. Enterprise API developers are captive developers who cannot simply switch over to another API provider, and the business relationship requires that they use the prescribed APIs.

The API management runtime must integrate with identity management systems, and support existing B2B security relationships that include security protocols and certificates.

Phase 4: Run

The runtime phase involves the operational delivery of the APIs, including servicing API calls, delivering content, and executing transactions.

Consumer APIs tend to be few in number but high in traffic volume, across large geographical areas. The security requirements for consumer APIs tend to be simple – typically user name and password for user authentication and an API key in the form of a shared secret for client authentication. User and client repositories are usually stored in a standalone database within the delivery platform, as the API consumer population can be very large, unverified, and have a high level of turnover. Consumer APIs usually require just enough throttling and traffic control to ensure that the quality of the API service is not negatively impacted by excessive users.

Enterprise APIs are usually consumed by business partners, and those partners and users are usually managed by an existing partner management system. The API runtime environment needs to integrate with these partner management databases to make runtime decisions using partner profiles, user roles, and service contracts. It is important to note that the management of partner and user information is handled by sales or support organizations and the user on-boarding tools they deploy, not by developers via a developer portal. Both the API consumer and provider organizations generally have some level of identity management infrastructure that is responsible for managing credentials.

The API management runtime must integrate with identity management systems such as CA SiteMinder, IBM Tivoli Access Manager or Oracle Access Manager. API runtime needs to support existing B2B security relationships that include security protocols and certificates such as an SAML tokens and X.509 certificates. Enterprise APIs are often bound by business contracts and SLAs. Therefore, advanced throttling, metering, and quota management capabilities are required to enforce contract terms.

Phase 5: Monitor and bill

The monitoring and billing phase is about measuring the usage of APIs and execution of the revenue cycle.

The monitoring requirements for **consumer APIs** tend to focus on usage statistics, to help business users understand the levels of service adoption and provide feedback for experimentation. Services delivered by most consumer APIs are free, so billing is usually not a significant requirement. Since consumer APIs do not transmit sensitive data, the typical auditing requirement is minimal or non-existent.

Enterprise APIs usually have much more stringent monitoring and auditing requirements. In addition to usage statistics for business analysis, enterprise APIs require rigorous and accurate transaction logging to meet compliance requirements and to provide evidential audit trails. Real-time monitoring and alerting on service levels are often implemented to uphold SLAs and avoid any penalties. Finally, detailed usage logging and service level measurements need to be delivered to billing systems to complete the revenue recognition cycle. This requires not only integration with billing systems, but also with partner management systems.

Enterprise APIs require rigorous and accurate transaction logging to meet compliance requirements and to provide evidential audit trails.

Your API management platform architecture

Fundamentally, your API management platform architecture will be driven by:

- The type of APIs you need to deliver
- The readiness of your source APIs
- Integration requirements

With cloud, mobile and social media now mainstream computing concepts, consumer and business users all demand access to applications and data from multiple devices, inside and outside the enterprise, 24 x 7 x 365. This means users will interact with your enterprise through many different interfaces, and those interfaces all converge at the API layer. A flexible and powerful API management platform that fits your business needs can create differentiation and help you compete in the "API economy." But first, you must understand the types of APIs you need to deliver and consume, and the sources of those APIs. Then, the 5 phases of API management and the required technology information in this white paper will help you on the road to building a comprehensive API management platform.

Learn More

For more information on API Management, go to Axway.com.

For More Information, visit www.axway.com