CRAMER
Amdocs OSS Division

THE NEXT GENERATION:
HOW DOES IMS AFFECT OSS?

CONTENTS

1. INTRODUCTION

1.1 WHY IMS?

Competitive pressures, exacerbated by the easy availability of free services via IP, have turned the telecommunications industry on its head. Throughout the industry, the imperative for change is well understood.

This is driving investment in infrastructure and supporting systems that enable delivery of new content-based services. Specifically, this means network initiatives in the areas of fixed-mobile convergence, NGN, SDP and IMS.

Along with the associated TISPAN, IMS is a standard that's gaining in popularity. According to *OSS Observer*, up to 150 service providers are currently engaged in IMS projects. IMS offers a standards-based approach that promises to truly allow the economical construction and delivery of so-called 'new' services from 'lego-block' components over 'any' technology to 'any' device.

There is much discussion and debate over IMS and its current state of development, which we will not go into here. Suffice to say, the need to support regular and ongoing development, delivery and assurance of high volumes of new services – and to do it conveniently, cheaply, creatively and commercially – is critical and will remain so in the foreseeable future.

1.2 NEW SERVICES MEANS TIGHT MARGINS

Most accept that regardless of protocol – for example, VoIP or VoIP via IMS – new services will be subject to competition from low-cost, non-traditional providers. This makes them highly price-sensitive, with cost being critical to profitability. As an analogy, consider the impact of fallout in a fairly typical service fulfillment scenario (see breakout box). Where services are price-sensitive, control over costs is essential to profitability. Operations are critical to that equation.

FALLOUT HAS 3 MAIN IMPACTS ON COST:

1. Cost of manual handling of fallout.
2. Delays in service delivery that can result in reduced customer satisfaction and churn – which means immediate lost revenue and necessitates costly new customer acquisition.
3. Introduction of errors through manual intervention, which in turn increases fallout rates.

A recent study commissioned by Cramer, Amdocs OSS Division, found that fallout rates of up to 10% are common. At that rate, margin is quickly eroded where pricing pressure is high:

> When delivering 10,000 service orders, 10% is 1,000 orders. Under IMS, we can estimate approximately 10% of those would require manual handling. If manual handling requires just one hour (at a full FTE rate of USD55 per hour), the cost is $5,500 per 10,000 orders.

> If 25% of manual fallout require site visits – a reasonable estimate – add an additional $12,500 per 10,000 orders. Again, if volumes are increased, the cost increases.

When you take into account that in reality, the volume of services under IMS is likely to be on the order of 10,000 *per day*, then the economics of managing fallout become significant.

2. WHAT DOES IMS MEAN?

2.1 HOW DOES IMS AFFECT THE NETWORK?

The IP Multimedia Subsystem, IMS, is an architectural framework. It was originally designed by the wireless standards body 3GPP for delivering IP multimedia services to end users. This idea was updated by 3GPP, 3GPP2 and TISPAN, which provided requirements for support of non-GPRS networks such as wireless LAN, CDMA2000 and fixed line.

From an operations perspective, the key differences between IMS and existing protocols are:

> ABSTRACTION

IMS abstracts service creation from service delivery. Potentially, this give you greater flexibility to take a wider range of slightly differentiated services to market. This allows you to appeal more directly to more tightly defined market segments in order to increase your market share and – perhaps more critically – your wallet share. Flexibility comes from the ability to componentize services and construct different options in a 'plug and play'-style environment. However, this also means that demand is less easily forecast by traditional means. In particular, managing peaks in activity becomes less predictable from outside. The ability to manage quality of service (QoS) cannot be a separate discrete activity, then, but must be inherent in operational processes.

> DISTRIBUTION

IMS allows customers to order *and* activate services directly via self service. This gives customers greater control and near-instant gratification since, in many cases, they can take delivery of a service when it's ordered. This contributes to greater customer satisfaction and potentially lower customer churn. At the same time, though, this direct access makes the network itself more complex. Touchpoints become distributed rather than centralized, which means the ability to manage capacity must be 'embedded' in operational processes, rather than driven manually from above.

> COMPLEXITY

IMS makes it easier for customers to order a service directly to the device where the service will be consumed. This helps promote greater consumption of services. (Why not order another video when it's so easy and so immediate?) However, ease of use for the consumer – and for product managers who dream up new services – corresponds to rising complexity in the network and in operations. Management processes need to be 'built-in' to functional processes and also automated, so the network can handle anything that's thrown at it, from nearly any direction – and do it on the fly. In particular, since new IMS-based capabilities are software-based, version control becomes an issue. A combinatorial explosion of versions needs to interoperate, so services can be managed according to multiple policies and delivered to multiple devices. This situation will also continue to grow over time.

2. WHAT DOES IMS MEAN? (CONT.)

2.2 HOW DOES IMS AFFECT OPERATIONS?

It has been suggested that IMS limits the need for OSS because many operational aspects of service management will be taken care of automatically in the network. However, as more service providers engage in IMS trials and start to go to market with IMS-based services, evidence is proving the opposite. The particular requirements of IMS actually make OSS more necessary, not less, to the delivery of IMS-based services.

In particular, OSS needs to be fully automated – able to handle those issues through interrelated planning, fulfillment and assurance functions. If it isn't, it is simply not possible to make money from IMS implementation.

> "IMS success cannot be achieved until a solid information management strategy and OSS/BSS alignment have been put into place."
>
> — STRATECAST, 2007

3. OSS FOR IMS

3.1 IMS MAKES OSS MORE IMPORTANT

IMS impacts OSS in three important ways:

> IMS makes efficient operations imperative.

The requirement to allocate, activate and assure physical and logical resources for delivery of a service is still necessary, at least in the first instance, and must be done as cost-effectively as possible.

> IMS brings new requirements to operations.

These need to be met in order for services to be planned, fulfilled and assured. Operational software is the logical place to address these requirements.

> IMS makes tighter cohesion within OSS mandatory.

For IMS services to be fulfilled and assured, and for both capacity and QoS to be ensured for those services, key operational processes must be interrelated to a greater extent than ever before. This is only possible from one integrated OSS platform, based on one integrated schema for both service and resource management.

3.2 IMS MAKES EFFICIENT OPERATIONS IMPERATIVE

Whatever else changes under IMS, at some point there is still a requirement to perform 'traditional' operational functions that allow networks to be planned and built, resources to be allocated and activated, and services assured. Next-generation initiatives such as IMS are arguably being driven by the economics of new higher volume, lower margin services. These same economics mean operations also need to be tighter, more cohesive and more cost-effective – or, in a word, automated.

In our view, OSS has to provide a platform that spans all functional requirements of operations including planning, fulfillment and assurance, for all technologies and all services. Crucially, these functions should be built around a single schema – an integrated service and resource inventory. Its scope is any network and any service.

An inventory-centric approach makes operations more efficient in two ways:

> With a single source of information across all functions, data integrity and consistency is more cost-effective. It also enables higher productivity by minimizing the additional cost and re-work caused by errors due to inaccuracies.

> Inventory-centric operations processes use data centrality to drive synchronization and consistency across operations, reducing errors. More importantly, this has a significant impact on the quality of the customer experience and also on the service provider's cost base, due to tighter optimization of network resource usage. It also results in faster fulfillment and more effective problem resolution processes. All of this helps perpetuate a virtuous cycle. Usage of the same base inventory schema in planning processes means that the inventory is created as the network is designed. This same inventory is used by fulfillment to determine the customer configuration, which means that the inventory is kept up-to-date by playing an active role in automating the fulfillment process. In turn, that means the output of fulfillment is a complete and current service and resource inventory, which can then be used with full confidence in assurance processes to detect and repair faults faster and more efficiently.

INVENTORY-CENTRIC OSS
CREATES THE VIRTUOUS CIRCLE

With IMS, existing traditional operational processes also need to take the following into account:

> IT MANAGEMENT
Many resources at the IMS Control Plane and also at the Service or Application Plane run on IT platforms, and these require very high availability and resilience. All IT resources, infrastructure, storage and applications require management, activation and configuration, in much the same way as network resources. It therefore becomes more efficient and effective to manage IT resources and network resources via the same schema.

> PRODUCT MODELING
The IMS vision requires rapid service creation and execution from reusable components, with strong automated support for service definition and launch. Operations need to be able to track, manage and control component implementation as an integral part of operations processes.

There will also be significant challenges in delivering services across a converged platform, and even greater challenges in migrating from legacy networks and service to IMS-based next-generation networks. The IMS vision will be delivered progressively over the next three to five years. Post-migration, challenges will occur in delivering convergent services on fixed, mobile and wireless access networks. The flexibility to model and manage services across multiple technologies is critical to supporting both legacy and next-generation services and networks, both in migration and in converged operations.

3.3 IMS BRINGS NEW REQUIREMENTS TO OPERATIONS

Essentially, there are four main operational requirements around IMS, where the ability of the OSS to specifically address the IMS environment becomes critical:

> Service management and fulfillment

> Policy management

> Device management

> Subscriber management

3.3.1 SERVICE MANAGEMENT AND FULFILLMENT

As discussed previously, there are implications for OSS in performing traditional resource-based fulfillment. For example, a service such as broadband has resource requirements that must be addressed.

In addition, OSS must track, monitor, configure and manage IMS-specific equipment as part of the fulfillment process, such as HSS and policy servers.

When a service is being deployed with no resource activation component (e.g., voicemail), IMS has a bigger effect on the service activation process. Here, the provisioning process for services 'should' be light on operations – all that is ostensibly needed is for the HSS to turn the service on and associate an instance with a particular subscriber. However, each service and each service instance also needs to be associated with a particular QoS to make it work. For example, a customer with a 'gold' package will have a 'gold' service level agreement to match. OSS is required to make that link explicit at the time of provisioning.

3.3.2 POLICY MANAGEMENT

Within the next-generation network architecture, operators must be able to control their subscribers, the services/applications they provide and the underlying network that supports these services. Policy Management is a fundamental capability that allows operators to manage the resources within their IP network and to provide hard performance guarantees for services like VoIP and IPTV. Policy Management needs to be supported by BSS/OSS, so policies can be created and managed throughout their lifecycle – from service creation through to service fulfillment and activation.

Policy Management can be deconstructed into a number of logical entities that include the policy decision, policy enforcement and charging functions. These capabilities provide the following real-time capabilities:

> Enhanced policy control that allows the operator to perform service-based QoS policy control for session-based packet-switched applications.

> Flow-based charging control, supporting charging models based upon volume, time and events or combinations of these.

To define policy and charging control, an environment that supports the creation and management of policies is needed. The creation of policies requires a number of inputs, ranging from the definition of the service requirement (performed within SLA management) to how the IP network is modeled and what QoS technologies are employed to support the service. The creation and management of policies should support the following functions:

> An inventory of policies that can be stored, retrieved and searched.

> The construction and viewing of policies allowing reuse of existing policy templates.

> Policy validation involving syntactic and semantic checks.

> Off-line conflict resolution for new policies that impact existing ones.

> Policy provisioning – for example, applying policies to network entities.

3.3.3 DEVICE MANAGEMENT

The delivery of next-generation services makes the ability to manage an end-user device increasingly important. As the number and sophistication of these devices grows, it becomes necessary to have a management solution integrated within OSS. As we have seen, the protocols to support device management are not consistent between definitions of next-generation architectures. Even within the same industry, there may be regional variations.

Service enablement is more productive when the inventory of devices, the non-application software (e.g., the operating system) and the applications it can support are all in one place. For example, service activation can become less prone to failure if end-device capabilities are recognized earlier in the service fulfillment lifecycle.

From an OSS perspective, the main requirements for Device Management (DM) are:

> PROVISIONING
Whether the device is provisioned through a DM server, smart card or enterprise server, the inventory must record and manage the process from customer care through activation.

> CONFIGURATION MAINTENANCE/MANAGEMENT
Device configuration parameters need to be stored and managed. The relationship between the device inventory, configuration inventory and DM server also needs to be maintained.

> SOFTWARE MANAGEMENT
In this sense, we refer to application/service software that can reside on the device. The DM server requires the software/hardware inventory of the relevant device.

> FAULT DETECTION, QUERY AND REPORTING
The customer care or help desk function requires visibility of key device characteristics.

> NON-APPLICATION SOFTWARE DOWNLOAD
This could apply to the device operating system, drivers, connection software and firmware. When faults are detected with this type of software, it's better to download a new set than to recall the device. An inventory of this type of software needs to be maintained, with a relationship to the device inventory and DM server.

3.3.4 SUBSCRIBER MANAGEMENT

Within the domain of Business Support Systems (BSS) such as CRM, the need to maintain one source of customer data has been clear to service providers. Within the domain of OSS, the need for centralized customer data has been less clear, and the focus of interest has been the network. However, IMS can allow customers to use a multitude of services, each with its own policies, and potentially on multiple devices. The need then arises to maintain one central source of data. That way, providers can manage all service provisioning, identifications, authentication and authorization, and billing data in one place – so interactions between a customer's services, policies, devices and versions of each can be managed and maintained with consistency and accuracy. The HSS supposedly can provide that single source. However, the HSS cannot maintain histories, so the functionality of the HSS has to be augmented in order to support a complete customer experience.

4. IMS MAKES TIGHTER COHESION WITHIN OSS MANDATORY

4.1 BRINGING IT ALL TOGETHER

With IMS, the interrelationship between operational processes is no longer merely desirable, but necessary. This is where it has its greatest impact on OSS.

In the service fulfillment process, for example, each service and service instance must be associated with a particular policy at the point of fulfillment. There is an implicit relationship between policy and services, and OSS is required to make that link explicit at the time of provisioning. It must ensure that the promised QoS is possible, and take rectifying action if not. This action could be immediate (e.g., reject request for service) or longer term (e.g., plan more capacity).

This also has implications for policy design. For an IP network, policy can be associated with two points for QoS on one service (A end and Z end), but cannot be assigned over the entire network. Short term, the realistic option is to manage capacity over access networks, and over-provision the core. However, this leads to higher capital expenditure costs than necessary, which will be unacceptable in the face of low- and decreasing-margin services.

Ultimately, OSS needs to take an 'upstream' role to make sure that the right type of IP network is available at the point of provision, compatible with the service being ordered. Planning within operations has to take on a bigger role and greater responsibility and, critically, network plan and design must take place commensurately with service design.

Going a step further in the provisioning process, the diversity of devices – such as handsets, set top boxes and different varieties – mean that there must be a linkage between the capability of a device (e.g., screen resolution) and the QoS experience. OSS needs to manage this linkage. What's more, it needs to do so where a device can run multiple policies and multiple services concurrently.

For instance, a service such as video download might have a policy of commandeering all bandwidth for its duration. If the subscriber receives a phone call in the middle of the download, what should policy management do? Some would argue that the incoming call, on finding "no bandwidth available", should prompt the subscriber to buy more bandwidth to support the phone call – so the subscriber can take the call and continue with the download concurrently, albeit at extra cost. To be clear, this is precisely the situation that occurs when policies for different services execute in isolation. The policy for the VoD service is unaware of bandwidth needs for any other service. It simply takes all of it until the download is complete.

Subscribers are unlikely to agree that this approach makes sense. In fact, providers will likely find they need to manage dynamic policies so compatibility between multiple services can be maintained both inside and outside the service. OSS can play a role in managing compatibility of policies, enabling interoperability of services at the subscriber, service instance and device level.

4.2 VERSION CONTROL

Finally, all services and all policy will be encapsulated as 'software' – software on devices, content servers and policy servers, which by nature are likely to only serve a part of the network at a time. Even with a small number of services, this means there will be multiple servers and multiple devices, and once linkage between instantiations is taken into account (e.g., a 'gold' policy for subscriber A, who takes a service bundle including VoD, mobile phone and daily news service – each of which has its own policy definition), this means a great deal of software. All of which will be versioned according to device, service, policy – and then interrelated at instance level by subscriber. The version control problem is substantial and OSS is required to manage and simplify the situation into a workable environment.

CONCLUSION

IMS brings exciting new capabilities to service providers, enabling them to create innovative new services that are easy for customers to order and run. Immediacy and ease of use for customers, however, comes at the price of greater complexity in the network. Therefore, the ability of operations to support processes such as fulfillment and assurance becomes more important, rather than less. Operations must be more efficient and automated to meet both cost and volume realities for new services under IMS. Operations must meet new requirements, particularly to support service management, policy management, device management and subscriber management. More than anything else, IMS means that operations must be seamlessly interrelated. For existing networks, the old silo approach might be less than optimal. In IMS, it's simply unworkable.

APPENDIX A

IMS BACKGROUND

The IP Multimedia Subsystem is a technology that provides advanced services for 3G cellular networks. It was developed by the 3rd Generation Partnership Project (3GPP) as a collaboration established in December 1998. It was based on evolved GSM core networks and the radio access technologies they support.

The 3GPP2 group is using IMS as a base for their Multimedia Domain (MMD) architecture. This will allow CDMA2000-based access networks to provide third-generation mobile services. The 3GPP2 core definition follows the IMS definition closely but there are differences to allow for the differences in radio technology – for example, codec support.

The services supported can comprise audio, video, text, chat and a combination, delivered over the packet switched network. The basic IMS architecture has a number of network elements within it. This architecture illustrates that the signalling path and the data path traverse different network entities.

The network where IMS can be deployed can be broken into the following layers:

> ACCESS NETWORKS
> Provides access to the end point that can utilize a number of technologies, such as Radio Access Network (RAN) and Wireless LAN. The services offered by the IMS network should be access independent.

> USER PLANE
> This provides the user with the ability to send and receive multimedia data. Examples of network entities included in this plane are Media Resource Function Processor (MRFP) and IMS-Media Gateway.

> CONTROL PLANE
> This is provided by the SIP Layer and its support functions. This layer provides session control such as call set up and termination. Examples of network entities included in this plane are Serving Call Session Control Function (S-CSCF) and Media Gateway Control Function (MGCF).

> SERVICES PLANE
> This is provided by the application servers that host advanced services. Examples are the SIP Application Server and Presence Server.

TISPAN (Telecommunications and Internet Converged Services and Protocols for Advanced Networks) is seen as the bigger brother of IMS. It considers the fixed line environment and its additional requirements, and introduces additional subsystems to those defined within an IMS architecture. Whereas IMS deals with SIP-based services, TISPAN addresses services that can also use non-SIP messages, such as IPTV when channel hopping. The main additional subsystems are the PSTN Emulation Service over IMS (PES), the Network Attachment Subsystem (NASS) and the Resource and Admission Control Subsystem (RACS).

ABOUT AMDOCS

Amdocs combines innovative software and services with deep business knowledge to accelerate implementation of integrated customer management by the world's leading service providers. By delivering a comprehensive portfolio of software and services that spans the customer lifecycle, Amdocs enables service companies to deliver an *intentional customer experience*,™ which results in stronger, more profitable customer relationships. Service providers also benefit from a rapid return on investment, lower total cost of ownership and improved operational efficiencies. A global company with revenue of $2.48 billion in fiscal 2006, Amdocs has more than 16,000 employees and serves customers in more than 50 countries around the world.

For more information, visit Amdocs at www.amdocs.com

ABOUT CRAMER, AMDOCS OSS DIVISION

Cramer, Amdocs OSS Division, was formed following the acquisition of Cramer, a leading provider of operations support systems (OSS). The combined Amdocs-Cramer solution is unique in its combination of OSS and BSS, delivering complete visibility of the customer, the network and the service. This will help service providers transition from legacy to next-generation networks and systems, and rapidly launch new converged services that quickly turn network investment into service revenue.

Amdocs has offices, development and support centers worldwide, including sites in:

THE AMERICAS:

- BRAZIL
- CANADA
- MEXICO
- UNITED STATES

ASIA PACIFIC:

- AUSTRALIA
- CHINA
- INDIA
- JAPAN
- THAILAND

EUROPE, MIDDLE EAST & AFRICA:

- CYPRUS
- CZECH REPUBLIC
- FRANCE
- GERMANY
- HUNGARY
- IRELAND
- ISRAEL
- ITALY
- THE NETHERLANDS
- POLAND
- RUSSIA
- SOUTH AFRICA
- SPAIN
- SWEDEN
- TURKEY
- UNITED KINGDOM

For the most up-to-date contact information for all Amdocs offices worldwide, please visit our website at www.amdocs.com/corporate.asp

amdocs

© Amdocs 2007. All Rights Reserved. Reproduction or distribution other than for intended purposes is prohibited, without the prior written consent of Amdocs. Amdocs reserves the right to revise this document and to make changes in the content from time to time without notice. Amdocs may make improvements and/or changes to the product(s) and/or programs described in this document any time. The trademarks and service marks of Amdocs, including the Amdocs mark and logo, Ensemble, Enabler, Clarify, Return on Relationship, DDP/SQL, DDP/F, Intelecable, STMS, Collabrent and Intentional Customer Experience are the exclusive property of Amdocs, and may not be used without permission. All other marks are the property of their respective owners.

© Cramer Systems Limited, 2007
Effective Date: March 2007
Cramer and the Cramer logo, whether or not appearing with the registered symbol, are registered trademarks of Cramer Systems Limited. Any third-party products or company names referred to may be trademarks of their respective owners. This document is valid from the "Effective Date" shown and supersedes any previous issue. It contains summarized information that will be subject to periodic change and customers are advised to check with Cramer Systems that they are using the current version. Cramer Systems has made all reasonable endeavors to ensure that the statements contained within this document are accurate at the time of publication but cannot guarantee that the document is free from errors.