



WHITE PAPER

Building a Security Framework for Delivery of Next Generation Network Services

A white paper by the University of Southern
California and VeriSign



Where it all comes together.™

**+ Abstract**

The role of network operators has morphed from that of simple infrastructure providers to enablers of Next Generation Network (NGN) services. While this expanded role encompasses a lucrative and growing market opportunity, operators now face new challenges regarding security and privacy in the delivery of these services. Threats range from the nuisance of spam to the propagation of viruses and more serious forms of identity theft and intellectual property rights violations. Invariably, new threats are introduced by the various service providers and consumers who use the NGN platform, but the burden of this increased risk is borne by the operators. Since NGN operators serve as the focal access and delivery point for communications, the design of a comprehensive security framework is critical to their business and ongoing relationships with their subscribers, service providers, and partners. The three main elements to be addressed by the framework are authentication, provisioning, and delivery.

The focus of this paper is to provide guidance in developing a framework for secure VeriSign® Intelligent Communications, Commerce, and ContentSM (IC3SM) services. By building a secure framework for authentication, provisioning, and delivery, operators may begin to realize the vast revenue potential offered by an NGN platform.



CONTENTS

+ Introduction: A New Transaction	4
+ The Emergence of NGN	4
Opportunities for Network Operators	5
Challenges for Network Operators	6
+ Building a Security Framework	7
A Layered Approach	8
Security Policy Considerations	9
+ Secure Communications, Commerce, and Content	11
+ Appendix A	13
+ Appendix B	14



Introduction: The New Transaction

For most network operators, the demand for NGN services introduces entirely new elements to the transactions they normally conduct with customers and partners. Below is illustrated a seemingly simple transaction—downloading video or music clips to a mobile phone—but beneath the surface, a sea of complexity looms for the network operator. These complications relate to the proliferation of new devices, authentication, provisioning, and delivery—and the crucial security and privacy issues that must be considered for each step.

A subscriber registers for a new service, such as music or video clips via a mobile phone account:

- *Operator must have method for authenticating the subscriber's identity and access privileges.*

The subscriber goes to the operator's portal to sign-on and shop for video clips:

- *Operator must be assured that the requesting device is free from all forms of malware as it connects.*

The subscriber may need to download an application to access and interact with video clips:

- *Operator must ensure such applications have been developed and deployed consistent with its security policy.*

Subscriber searches for and requests a video clip to download:

- *Operator must have relationships with third-party content providers to ensure a compelling catalog, while providing a convenient single-sign-on experience for the subscriber.*

The service is provisioned to the subscriber:

- *Operator must confirm the privileges of the subscriber and maintain their privacy while facilitating the transaction between parties (including billing and clearing).*

The video clip is delivered to the subscriber's device:

- *Operator must be able to deliver the content to a variety of devices (from mobile phone to set-top box or PC) while enforcing and protecting the digital rights associated with the content.*

The Emergence of NGNs

It's not your father's telecommunications network anymore (it may be said however, that it is your teenager's network). No longer do consumers and businesses accept the limitations of single-use devices or networks—both individuals and businesses want the ability to communicate, work, and be entertained over any device, any time, anywhere. The demand for these services, coupled with innovations in technology, is advancing traditional telecommunications far outside its original purpose. The revenue opportunity for network operators is potentially huge, but along with this potential comes risk. To enable network operators to reap the benefits of NGN services, the risks must be addressed with technology solutions that provide security, efficiency, and desirable services for the emerging marketplace.

IDENTIFY POTENTIAL RISKS

- User identity theft
- Application identity theft
- Network exposure to third-party applications
- Information disclosure
- Denial of service
- Unauthorized capture and distribution of content
- Inability to maintain data integrity
- Inadequacy of security standards
- Improper security design of NGN service platform
- Traditional enterprise security risks
- Business continuity
- Unauthorized services-revenue leakage
- Unauthorized or non-secure (malware) applications

Advances in telecommunications and Internet-based technologies have led to the integration of previously analog-only, circuit-switched technologies with newer, ubiquitous packet-switched technologies. These new broadband networks are expected to carry a number of services, including streaming video and audio, Voice-over-Internet Protocol (VoIP), Push-To-Talk (PTT) applications, interactive games, and organizational and commercial transactions. Largely characterized by packet-switching technologies, these NGNs operate over telephone, cable, satellite, and mobile networks. There are three main types of innovation fostering the growth of NGNs:

- **Smart Devices**—In the past, a device served a specific purpose: the television for entertainment, computers for work-related productivity, personal digital assistants (PDAs) for personal information management, and mobile phones for communication and mobility. As technology advances and consumer demand encroaches, these boundaries are crumbling and giving rise to multi-use devices. Today, people expect to be entertained through PDAs and mobile phones as much as they use their computers for personal communication and mobility. As an industry, we have a chance to learn from the lessons of the PC industry (inadequate security) and ensure that the NGN embodies the virtues of an end-to-end, seamlessly secure user experience.
- **Application Simplicity**—Consumers and companies seem to prefer a single, simple, and secure interface to access multiple applications or contents, such as mobile banking or a music portal. This demand, in combination with the adoption of client/server architecture and protocol standardization, has led to the emergence of Web browser-like clients as the ubiquitous user interface. The desire for simplicity and enhanced, personalized user experience is placing the burden (and opportunity) with network operators to be the one source for services delivered through a trusted service provider.
- **Flexible Infrastructure**—Until very recently, infrastructure was built for specific purposes for particular industries that were regulated and demarcated. Today, virtually any medium can support any service—voice, video, and data are available through cable, wireless, and/or telephone networks. This change requires a more flexible, more intelligent infrastructure that can scale, adapt, interoperate, and secure all the information required to deliver services.

Because of these three areas of evolution, today's NGNs are defined more by the services they support than by traditional demarcations of physical infrastructure, i.e., Verizon is no longer a "phone company," but a provider of communications services. These network operators, who support the physical infrastructure and provide the platform for new services, will continue to play a central role in the evolution and future success of NGNs.

+ Opportunities for Network Operators

With many technological limitations and regulatory restrictions lifted, network operators are now in a position to offer and support NGN services and potentially reap the benefits of the new market. The benefits are many and may include the following:

- Operational efficiencies due to unification of multiple networks and potential ability to scale at a lower cost
- Improved customer service by providing self-care abilities and lessening the burden on care centers
- Increased speed to market and rapid launch of new services by leveraging open standards and existing infrastructure

- More rapid return on investment due to reduced operational overhead
- Increased revenue and loyalty opportunity by selling new services and content portfolio provided by third-parties that conform to the policies of the NGN operator

New opportunities are encouraging network operators to look beyond their core physical offerings to better serve their consumer and business customers. Recent examples include SBC (a network operator) teaming with Yahoo! (a content provider) to provide consumers with a bundled Internet experience instead of separate Digital Subscriber Line (DSL) and Internet Service Provider (ISP) services. Similarly, many network operators are working with enterprises to provide a bundle of NGN services. For example, Sprint manages the bank ING DIRECT's needs by bundling Internet protocol (IP) services such as Virtual Private Network (VPN), wireless access, and VoIP with firewall and intrusion detection services.

+ Challenges for Network Operators

In their transition from providing only infrastructure to providing NGN services, network operators are facing an array of challenges. Business challenges include new pricing structures, new relationships, and new competitors. Technical challenges include migrating and integrating with new advances in technologies from fiber-optic installations to Wi-Fi support. Among those is the very significant undertaking of developing a comprehensive security policy and architecture in support of new NGN services.

Network operators are newly facing the need to protect and manage the identity and privacy of their users according to legal and business mandates, and to protect copyrights and digital rights for music, movies, games, and ring tones. Offering copyrighted music ring tones is just one example. Others include a network operator that wants to add a new content provider's catalog to their portfolio of music or video, or content around a local event such as a ballgame. In each of these cases, they face obstacles that can potentially lead to low or no adoption of the new service. The following lists just a few of these issues:

- Subscribers may not fully trust the third-party partner and/or its management of their privacy.
- Sharing information raises privacy issues and increases liability risks for the operator.
- Subscribers may find it cumbersome to register for individual services and be required to repeatedly provide personal information.
- The owner of the copyright (record label or other content provider) might not be comfortable with a digital rights management (DRM) system used by a network operator.
- Sharing location-specific consumer information with partners may violate local and state privacy laws.
- Mobile devices are easily transferable and adult content is widely available so mechanisms to ensure age verification or provision of parental controls are needed.

A fundamental problem with the prevailing approach to managing security of NGN services is that it is piecemeal and often technology-driven, i.e., a bottom-up approach where software or a set of technological tools broadly dictates the security framework to be implemented. While this semi-centralized approach has some benefit in the form of corporate security standards, it is not suited to the dynamic nature of NGN services. In summary, a network operator's NGN platform requires a radically new approach to service delivery.

Building a Security Framework

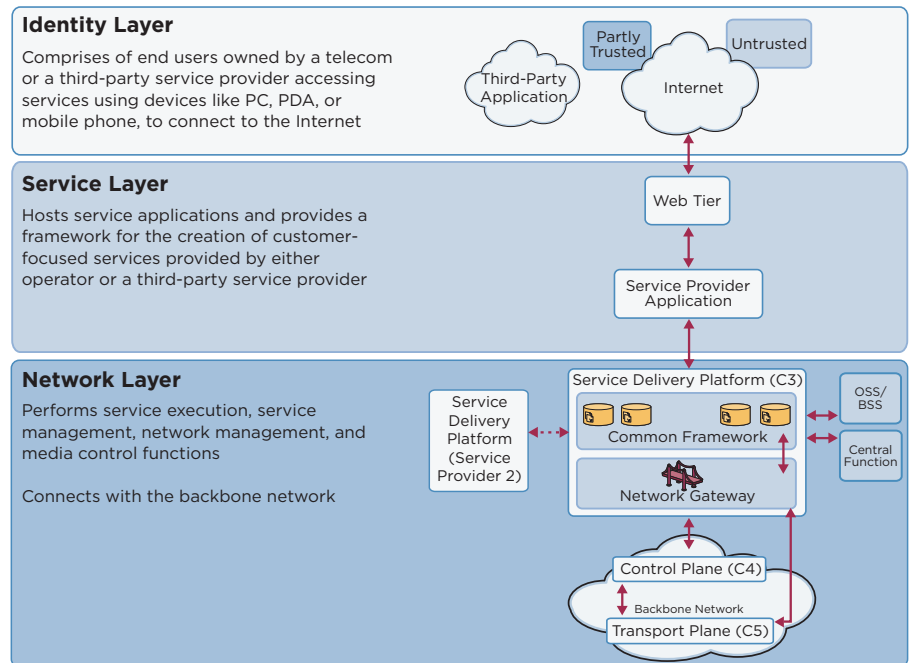
FIVE PRINCIPLES TO PREVENT SECURITY BREACH

- Know ALL the access points, access modes, and access methods to your NGN to identify vulnerabilities
- Verify your users before allowing access to NGN services—if needed, employ multiple levels of verification
- Know the access and usage privileges of your NGN users—have the ability to dynamically grant and revoke privileges
- Periodically analyze access patterns and usage behavior—use this information to fine-tune access, authentication, and authorization
- Maintain a record of all patterns of access, authentication, and authorization—make sure this record matches with specific compliance requirements

The overall security framework can be broadly described as a reflection of an enterprise’s comfort level with the various activities that comprise an NGN transaction. Attacks on NGN transactions, through viruses and worms, are dangerous to operators and all of their customers. In 2001, NTT DoCoMo was hit by a virus that directed their phones to call 110 (Japan’s 911) when users opened email. Just last year, a Trojan horse program attacked PocketPCs with malware that gave the perpetrators control of the devices. Recently, T-Mobile subscribers in the United States were hit by the Commwarrior worm. Phones infected by this worm searched for other phones that could be reached over Bluetooth® technology and sent infected files. In addition to other spreading over Bluetooth, the Comwarrior worm also read the local address book on the phone and sent unsolicited Multimedia Messaging Service (MMS) messages containing the Commwarrior files. As it was for the Internet and e-commerce, security is often cited as a top reason for enterprises and individuals to avoid new communications services.

While the consolidation of NGN services through the network operator makes services simpler for the end user, the operator faces new complexities. The basic structure of an NGN transaction contains three layers—the identity layer, the services layer, and the network layer. Each of these layers requires a corresponding level of security to ensure a secure, end-to-end transaction.

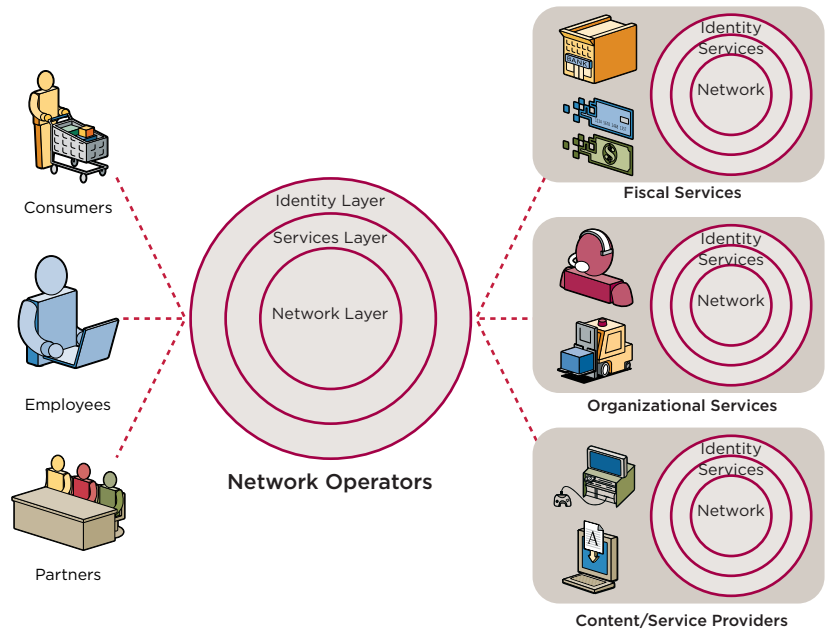
Figure 1: NGN Deployment



+ A Layered Approach

Instead of a technical or architectural focus, we recommend the framework be approached from an activity-based-solution perspective so the operator can control each layer within a comprehensive security framework. As shown in **Figure 2**, the complexity is high and security must be addressed at every layer and at each step of every layer.

Figure 2: Layered Approach



- **Identity Layer and Security Level 1 (S-1)**—This layer is concerned with the management of customer identities and forms the basis for interaction between the network operator and the end user. As the primary gateway, it serves as a mechanism for acceptance or exclusion, i.e., who should be allowed, what devices should be prohibited, etc. When a subscriber logs on to an operator’s portal, the operator must authenticate the identity of that subscriber. The operator also must help ensure that the device used to connect to the network is free from malware and in compliance with security guidelines for accessing services. The integrity of the code and application that is running on mobile devices are of paramount importance. The operators need to allow only trusted code and applications to be downloaded to the mobile devices. The Identity Layer and S-1 is the first line of defense, so any viruses or worms must be thwarted at this level, as well as strict controls in the form of device and application security policies enforcement must be exercised.
- **Service Layer and Security Level 2 (S-2)**—The Service Layer and its corresponding security level define the content and services allowed based on the subscriber’s access rights and privacy and preference settings. Instead of asking their customers to trust an assortment of third-party content providers, network operators may instead offer a method of access to a library of content and services (off-portal access) that does not require the subscriber to register with each provider individually. At this layer, the operator would also provide the infrastructure for pay-per-use billing so no additional

RECOMMENDATIONS FOR SECURITY MANAGEMENT OF NGNs

Mobile Security

- Personal firewall, anti-virus, and data encryption capabilities for the mobile devices
- Secure remote VPN access from the mobile devices for the corporate access or to access other services such as mobile banking
- Automatic near real-time encryption of data, e.g., emails and text messages stored on the device, memory cards, and during transmission
- Security policy enforcement for the mobile devices, e.g., access control of peripheral usage, including secure digital (SD) cards, infrared (IR), Bluetooth,[®] and USB ports
- Enforce basic minimum anti-virus feature before allowing an access to services
- Ability to download software and applications that are trusted (e.g., digitally signed and revocation checked) and only from trusted and audited sources

Content Protection

While service and application/operating systems providers are responsible for content protection, the mobile operator should only be responsible for secure delivery and appropriate DRM usage.

Secure Location-Based Services (LBS)

Locate the LBS infrastructure in a secure environment and have threat and vulnerability protection in place. User privacy and preferences should be major consideration for all LBS service delivery. Only appropriate information is to be shared with service providers.

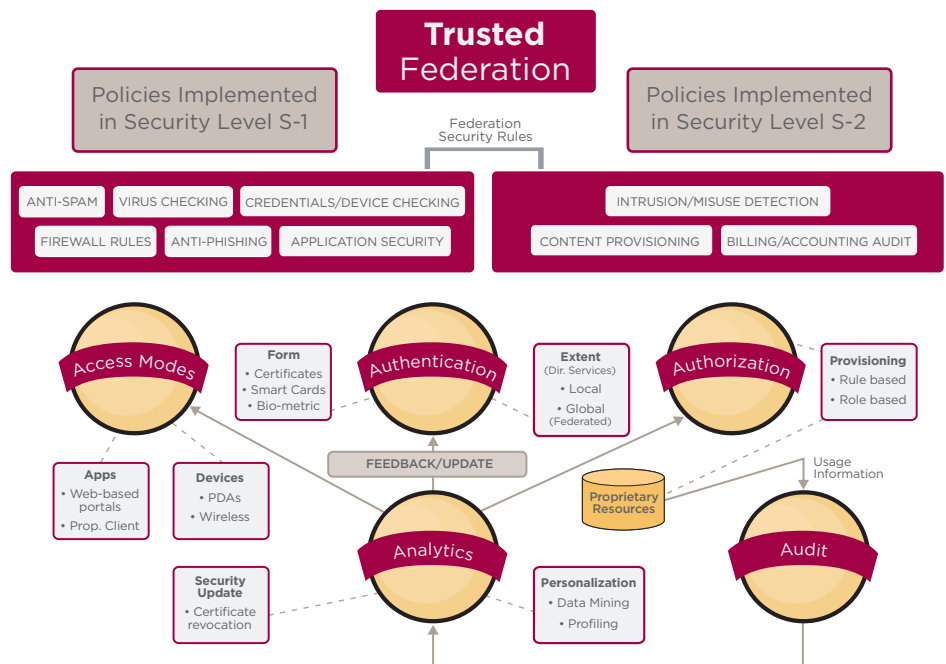
financial and personal information is requested from the subscriber. When the operator (a known, trusted quantity) acts as the mediator, it protects the privacy and enhances the loyalty of the subscriber, thereby increasing the likelihood that a transaction will not be abandoned. By addressing security and privacy issues, operators are likely to see broader service adoption facilitating new revenue generation and improved customer loyalty.

- **Network Layer and Security Level 3 (S-3)**—This layer can also be referred to as the core network. While somewhat less dynamic than the other two layers, the technical interactions between the network operator and the actual delivery of services are determined here. This layer opens up the network to third-party service applications, enabling application developers to develop, deploy, and manage service applications through the use of common open-standard application program interfaces (APIs), which expose the underlying network functionality. While reducing time to launch new services and delivering efficiencies in managing services on an on-going basis, it presents a new set of security challenges. Security at this layer defines the trust relationship between the operators and a variety of third-party content and service providers, ability to accept trusted software content and programs, and helps ensure overall security of the infrastructure that is delivering these services (e.g., location-based services, PTT services and access to gaming sites) by leveraging core network functionality including Operations Support System (OSS) and Billing.

+ Security Policy Considerations

The following list defines areas of consideration and action for security policy as the five A's: access, authentication, authorization, analytics, and audit. **Figure 3** illustrates the factors involved with these five areas.

Figure 3: Trusted Federation



Trusted Federation

Mobile NGN operators should create their own federation or preferably identify trusted third-party federations to work with. Clear information sharing policies and identity profile management principles should be addressed by the involved parties. A trust infrastructure is required to ensure that the user lifecycle management is implemented in an environment consistent with standards-based and public Federation Identity Management specifications, such as those defined by the Liberty Alliance Identity Federation Framework and the Web Services Security Roadmap and WS-Federation specification. Identity providers (e.g., operators) and third-party service providers may be required to support these and other federation protocols as part of participation in a federation.

Standards Compliance

Mobile NGN operators need to maintain standards compliance across their service providers. Adherence to open standards regarding encryption (e.g., RSA, AAC, and digital certificates) and federation protocols (SAML, Shibboleth, etc.) is important.

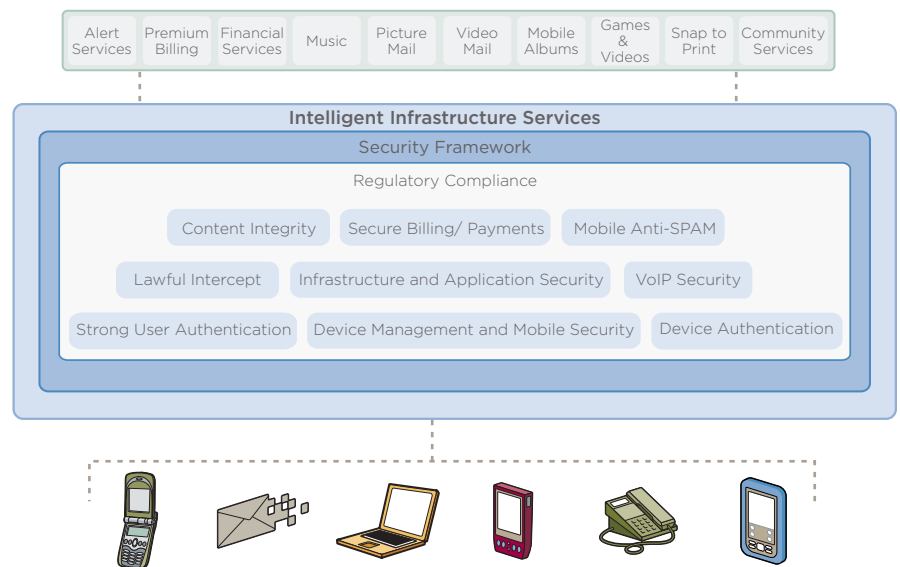
- **Access**—The first point of contact with an NGN operator is through the mode of access that a user employs. Not only do different devices have different levels of usability, but the security threats posed by each can be quite unique. Devices support a myriad of applications and variety of protocols, and determining the range of devices, applications, and protocols that a network operator will support is a critical piece in the design of firewalls, virus checkers, spam controllers, etc. While managing a single category of devices might be less complex, customers and service providers alike may drive the operator to support a combination of devices. Therefore, decisions about access must reflect both the operator's security policies and customers' and service providers' needs.
- **Authentication**—Authentication is the process of verifying that an entity (i.e., person, device, application, network, or agent) is indeed who they say they are. While decisions regarding the method of authentication are critical, care must also be taken not to discourage legitimate users. The operator will not only have to make important choices regarding the technical protocols employed here (i.e., Shibboleth®, SAML, etc.), but also concerning many non-technical decisions as to who authenticates, how many times an entity needs to be authenticated, and how many different combinations of authentication technologies are used. These decisions can be quite complex as they encompass various options regarding the type of proofs or credentials presented (i.e., password, codes, digital certificates, biometrics, location-based, GPS, etc.); the number of levels or factors required (i.e., strong or weak, single- or multi-factor verification, etc.); and the party that verifies (i.e., local or federated). Increasingly, the option of federated authentication, where a trusted third party constructs a trusted network (and entities need not be locally re-verified) is emerging as a viable option. Authentication is critical not only to ensuring content integrity but with increased deployment of Web-services, it will be an important factor in determining what operations will be allowed in the network. Due to an increasing number of phishing and other spurious content, verification of service providers on a dynamic basis (beyond initial trust) is crucial.
- **Authorization**—While decisions regarding the previous activities largely focus on who to exclude (or include) and play an important role in S-I, the authorization to use content, services, and other resources form the backbone of commercial transactions that take place on an NGN platform. Decisions at this level govern security policies, which help ensure that only the right entities have access to particular content. This authorization is granted simultaneously by both the service provider and fiscal entities, such as banks. And while it might be less complex to employ a one-by-one level of authorization, economies of scale often dictate a template or profile approach wherein rule-based or role-based provisioning might result in more manageable security policies, e.g. allowing premium and standard plans with associated privileges.
- **Analytics**—It is important to recognize that security policies cannot be static and they need to be constantly updated. Just as usage information is monitored and mined for better customer service, similar information can be obtained and employed for superior security policies. Most commonly, mining usage activities should play a direct role in vulnerability management and deployment of intrusion detection systems, including updating of firewall rules. Other systems, such as intrusion response and spam controllers, are also increasingly adopting analytics, such as Bayesian inference techniques, to dynamically update security policies. It is this type of intelligent infrastructure that can help to increase security in the most dynamic, effective manner by extending threat and vulnerability management to the mobile environment.

- **Audit**—Activities in this dimension have largely been dormant until recently when legislative action was taken regarding privacy protection and process management. Audit is simply an element of accountability, where security policies should reflect the systematic adherence to a set of established criteria. If an NGN operator supports kid-friendly services and allows sharing of profiles between its consumers and service providers, its security policy may need to reflect the requirements of the Children’s Online Privacy Protection Act of 1998 (COPPA). The need for security policies that reflect legislative and consumer demands is critical. Security policies should be equally concerned about internal threats (including an operator’s own partners) as much as threats from the outside world.

Secure Communications, Commerce, and Content

Security and privacy must be addressed in order to provide content access, monetize services, and enhance customer loyalty while improving average revenue per user (ARPU). As outlined in this paper, the best security approach to the delivery of NGN services will address all the existing and emerging risks with a security framework that enables the secure delivery of communications, commerce, and content services. **Figure 4** demonstrates how it should all come together and address the myriad issues within an intelligent infrastructure for security.

Figure 4: Security Framework for NGN



NGN services are potentially the largest opportunity for revenue growth that the communications industry has seen since the cellular phone. But like it was for the Internet and e-commerce, security is the primary obstacle that must be addressed to ensure acceptance and proliferation among business and consumer customers. VeriSign, with a proven heritage in Internet security and telecommunications services, is uniquely qualified to offer operators solid solutions for building a secure IC3 framework.

Contact VeriSign today at www.verisign.com to learn how our solutions enable operators to take full advantage of the opportunities provided by the emerging NGN services market.

+ Institute for Critical Information Infrastructure Protection (ICIIP)

Next Generation Networks provide technology enablers with new options and services. As the new service roles are being redefined, there are a host of security challenges facing the ecosystem partners. The security challenges range from push forward advertising like Spam and viruses to the more serious threats to personal identity and intellectual property. As in the PC world, the distribution of digital assets compromised by these threats can be introduced by personal users, insiders, partners, service providers and in the case of NGN, operators. This white paper takes a first step in developing a framework to define the potential problems and offer up alternative solutions to those inherent risks.

Yet, it must be remembered that security is not the sole responsibility of a single person, department or merely a technology application. Rather, Systemic Security Management, an approach to security that pays for itself, is everyone's responsibility and that responsibility needs to be extended throughout the organization through proactive planning, open communication, and work force commitment. Systemic Security Management is architecturally hardened, culturally supported, strategically implemented, extended beyond the enterprise boundaries and ultimately provides the enterprise with a competitive advantage.

ICIIP is an Organized Research Unit and Center of Excellence of the Center for Telecom Management at the Marshall School of Business, University of Southern California whose mission is to close the gap between the current corporate cyber security risk profile and what is needed to protect our nation's critical information infrastructure. ICIIP's strategy is to create business value for investments in information infrastructure security through public/private partnerships, education, and research while providing maximum insight and objectivity. ICIIP developed and conducts education and training curricula on "Systemic Security Management—Security that pays for itself" for classes targeting C-level decision makers. For more information on how to lead or implement Systemic Security Management for your organization, please contact Charles Meister at ICIIP at USC at 213-740-0980, cmeister@marshall.usc.edu, or http://www.marshall.usc.edu/web/CTM.cfm?doc_id=5356.

Appendix A illustrates a use case for the development of security policies for mobile NGN services.

Appendix B is a helpful checklist of critical factors to consider in the development of NGN services and policies.

Visit us at www.Verisign.com for more information.

Appendix A

USE CASE 1—NGN Security Policies for Mobile Operators

NGN mobile operators may choose to decide on the set of services that they support by having agreements with the service providers. Here the operators open up their core network only to these service providers. Alternatively they may adopt a more open approach where the users have the option to access a set of affinity groups by leveraging an operator’s portal. This approach is increasingly being deployed since it improves customer loyalty by offering subscribers multiple choices for off-portal access in contrast to the traditional “walled garden” approach. The best of both worlds, where usability and content is king, espouses an open approach which more closely reflects the NGN architecture—an approach that promotes innovation while ensuring consistent user experience through policy management and enforcement, helping to protect the billions of dollars in investment in NGN networks.

Walled Approach (Core Network Open to Only Selected Service Providers)
<p>Pros:</p> <ul style="list-style-type: none"> • Operators have more control over service providers. • Operators may choose to operate with only those service providers who have good data management techniques and maintain customer privacy. • Security is easier to implement since the operator knows beforehand the set of service providers to support. • Can help generate revenue by selectively choosing high-revenue services and service providers.
<p>Cons:</p> <ul style="list-style-type: none"> • Usability is greatly reduced. • Expensive to scale. • Revenue obtained may be less since only few service providers use the network.
<p>Security policy issues:</p> <ul style="list-style-type: none"> • Can control access modes and access devices. • Operators may decide beforehand on the type and level of authentication required for the different service providers and users. • Authorization decisions can be negotiated with the service providers beforehand. • Analytics operations can be reduced by carefully choosing service providers with whom the operator interacts. • Audit is simplified • NGN mobile operators can possibly dictate DRM solution to be adopted.

Open Approach
(Leveraging an Ecosystem of Content/Service Providers)

Pros:

- Open approach allows the operator to simulate “PC on a cell phone” environment.
- Helps improve customer loyalty, and creates an opportunity to monetize third-party access.
- Revenue generated may be higher since the set of service providers transacting is higher.
- Can support new service providers with minimal modifications.
- Spurs innovation and usability.

Cons:

- Need to build the eco system—requires a trusted third party.
- Operators have less control over the service providers.

Security policy issues:

- Complex security policies governing allowance of devices, applications, and other modes of access may be required as mandated by users and service providers.
- Authentication decisions are complicated due to the presence of multiple service providers and the dynamic framework.
- Federated mechanisms may be constructed for authentication and authorization.
- Analytics will be complex since multiple service providers use the network, and the system is dynamic.
- Audit mechanisms are complex since the operator may be interacting with previously unknown service providers.
- Security policies will be influenced by the service providers and the user concerns. Security policies are made more complex by the presence of legislation and dynamic network behavior.
- Service providers may dictate the DRM solutions to be deployed.

Appendix B

A Checklist of Critical Factors in Launching New NGN Services

Security Framework

- What are the specific security policies and solutions required for various layers, S-1, S-2, and S-3? Does the security framework address infrastructure, applications security, and privacy requirements? What are the auditing needs? What is the strategy to proactively monitor vulnerabilities?
- Are there specific regulatory requirements? Are there contextual sensitivity issues (e.g., might children be able access games with mature ratings?). Ensure compliance with specific legislations (COPPA, HIPAA, GLB, etc.)
- Are there special service guarantees, bandwidth assurances, etc. (e.g., does the content involve real-time delivery, intensive data transfer, etc.?). Ensure partnerships with appropriate edge-network partners.

Revenue Management Issues

- How will the new service be offered? Can pay-per-use pricing be supported?
 - Is the new service standalone or a bundled offering?
 - What is the revenue-sharing mechanism with the content provider?



- Can access to services and content be monetized?
- Can access to an ecosystem of third-party provided services and contents be enabled rapidly, in a matter of days?

Ease of Use and Personalization

- Can subscriber access content with a single click in a safe and secure manner?
- Can access be billed without significant integration efforts?
- Can service/content be personalized without compromising user privacy?

Content-Protection Needs

- Is content/service subject to intellectual property rights protection (e.g., will the content be pirated?).
- Can you ensure appropriate DRMs to be used in consultation with the content providers?

Technology Standards and Infrastructure Factors

- Are there new technologies involved?
- Consider changes to be made by:
 - End users/consumers (is a new device needed?)
 - Partners
 - Your network infrastructure

Customer Asset Management Issues

- Who owns the customer information?
 - Will full consumer profiles be shared with content providers?

Federation Management Issues

- If you are part of a federation, will the new service satisfy your federation's security framework?
- Can user profiles be transferred across the federation?
- Is your content provider willing to join the federation? Do you have access to an ecosystem of content and service providers?