

White Paper

By Martin Koistinen and Mike Watson, 2004

Contents

- 2 > Keeping Quality Customers Longer
 - > Single View of the Customer
- 3 > It all Begins with Trust
 - > Content Delivery Framework
- 4 > Authentication Flexibility
- 5 > Single Sign-On
 - > Managing Suppliers
- 6 > Common Services Gateway
 - > M-Payment Services
 - > Data Protection Services
 - > Specific User Profiles
- 7 > Security 'Baked' into the CSG
 - > Attacks from Supplier's Network
 - > Managing the Supplier Lifecycle
- 8 > Conclusion

Emerging mobile communication channels mean that network concepts of security are rapidly becoming redundant.

The shape of the mobile communications landscape is set to radically alter in the coming years. The advent of increased bandwidth is changing the way in which mobile operators carry out business, as revenue streams for information and data transfer gain greater importance. Increased bandwidth means new and larger applications and mobile devices that offer customers services such as picture messaging, video, games, transactional capability and e-billing.

In the context of mobile communication, security is about knowing your users and suppliers and not only enabling but also controlling their access to products and services.

These applications—provided by third-parties—are offered to customers using the mobile operator's infrastructure as a delivery network. This framework combines the infrastructure for the services and the business processes that integrate mobile operator and third-party business systems. Operators now move information for revenue, so it is not surprising that information security is essential. For example, companies who provide end-user services will rely on the security of the operator's network to maintain the integrity of the content they provide.

However, these emerging mobile communication channels also mean that network concepts of security are rapidly becoming redundant. The view that security is only about protecting the network's borders no longer holds water. In the context of mobile communications, security is about knowing your users and suppliers and not only enabling but also controlling their access to products and services.

Keeping Quality Customers Longer

Successful mobile operators understand that the key to exploiting the new mobile communication dynamic is to find ways to keep and increase the value of their customers by lowering the churn rate—which has historically been as high as 30 per cent for some operators—and to increase the Average Revenue Per User (ARPU).

Users, on the other hand, quite naturally have a completely different view. Whether in a retail outlet, on a handset, or on the Web the customer expects the operator to know who they are and accordingly to treat them as a valued customer. And, implicitly, they also expect airtight security.

For the operator, recognizing the value of a single customer, among what could potentially be millions, is the first and crucial step on the road to profitability. Absolutely central to this capability, is a single view of the customer that is accessible by all of the operator's agents in real-time and at any time.

Armed with this information, agents can identify quality customers and ensure they don't become the next to churn.

Unlike most businesses, a mobile operator has the opportunity to analyze its customers' behavior at the most granular level. For example, operators are already able to establish the call patterns of its customers—from time and duration to geographical location. This capability is enhanced as increasing numbers of users adopt applications enabled by wider bandwidth and use their mobile handsets to make purchases. In short, operators will be able to see what a customer is doing, when it is being done and how much is being spent—providing customer segmentation by value and enabling the offer of appropriate value-added services to these customer segments.

However, while this model represents the ideal, the reality for many operators is a fractured view of the customer. Many established operators have fragmented customer databases in different physical locations and logical data structures that use disconnected keys and indexes. Such a poor environment impedes the operator's ability to synthesize knowledge from the vast amount of available customer data.

Single View of the Customer

One of the most valuable projects such an operator can undertake is to wholeheartedly embrace customer relationship management and manage its customer data in such a way that it provides a single customer view. The ability to achieve this will, in many instances, determine how successful an operator will be in embracing the brave new world of mobile communications.

The single customer view is arguably the operator's most valuable asset. However, to provide unified access—whether for call center agents, via web-applications, suppliers, or even other subscribers—it is absolutely crucial that its use is controlled. It is also vital that all these parties and relevant others have this information in an unimpeded manner or the value of the information asset is reduced.

One cannot buy trust but one can invest in ways to protect it. A solid security infrastructure supporting audit processes and accountability is essential.

One of the key objectives for an operator is that its infrastructure must allow this access, in a controlled but rapid manner. An architecture that has security transparently “baked in” provides information to the right parties at the right times. With a well designed security model and supporting infrastructure, the operator can provide handset or web-based self-service for the customer.

This allows the customer controlled access to his or her own records for functions such as updating contact details, accessing billing information, changing security PINs, passwords and other shared secrets. Also when the customer calls for assistance the security infrastructure must prevent hijacking of the users’ accounts by call center agents. This is an important aspect in security design and, with proper care, misuse of customer information can be prevented.

It all Begins with Trust

There are many strategies for capturing and keeping high-value customers but one of the most effective is to build a trust-based relationship. If the customer trusts the network and its processes a sense of comfort and safety will be engendered and the customer will feed information to the operator, who will respond by providing clear value in return.

Successful operators will leverage a user’s profile to deliver the most relevant and personalized content, maximizing the revenue earned while simultaneously minimizing the cost. The relationship will last as long as both parties find value.

The longer the customer invests in this relationship, the more difficult it will become to change operators. The longer the user stays with the operator, the lower the customer’s cost to the operator. And it all begins with trust.

To the customer, a trusted operator protects all personal information from unauthorized parties and misuse. If the customer view is the operator’s most valued asset then trust is its most valued quality. Unfortunately, trust is hard to obtain and easy to lose. One cannot buy trust but one can invest in ways to protect it. A solid security infrastructure supporting audit processes and accountability is essential. Compliance with local, regional, national and international regulations is also crucial and should be factored into any security strategy.

Content Delivery Framework

A customer’s experience with a telecommunications provider today extends beyond the operator’s boundaries. Increasingly, operators rely upon products and content supplied by third-parties to provide the rich experience its customers have come to expect.

Managing this content is the role of the operators’ Content Delivery Framework (CDF). The CDF must not only handle content from separate sources, but also deliver it to multiple devices (see Figure 1). Customers already expect to interact with the network using their mobile handsets, their PDAs, personal computers and soon with their television sets as digital TV becomes commonplace.

The CDF is the ideal place to enforce access controls. To meet these goals, the CDF must be integrated into the security architecture and within this context it provides at least the following key benefits:

- > Prevention of unauthorized access to content
- > Seamless authentication of customers to the required assurance levels
- > Enabling the customers to manage their credentials and profile.

Since the range of services to the subscriber is broad, the level of assurance required for any particular transaction should be appropriate to the value of the assets it protects. For example, it doesn't make sense to require a digital signature from the subscriber for a ring tone download, any more than it does to approve a loan application with just a single password.

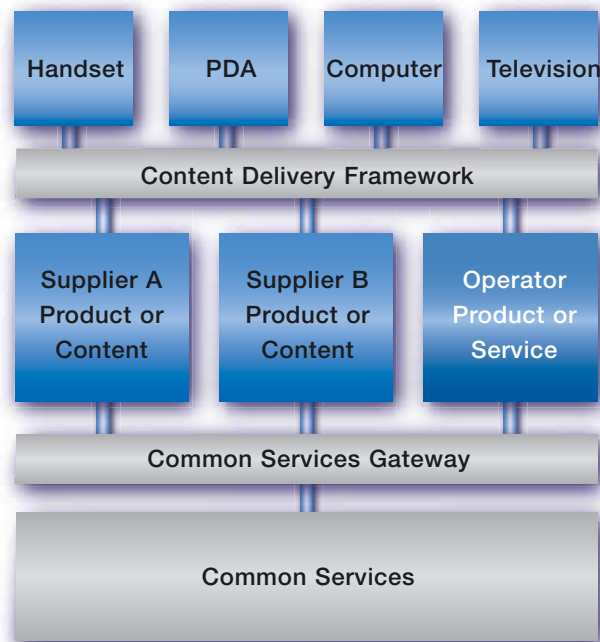


Figure 1 – Simplified view of an operator architecture

Since the range of services to the subscriber is broad, the level of assurance required for any particular transaction should be appropriate to the value of the assets it protects.

Authentication Flexibility

A robust security architecture permits multiple forms of authentication over a range of convenience and assurance levels. It also provides a number of expected customer features, such as single sign-on and alternative identities. By having a value of assurance assigned to each of these credentials, the system can minimize the number of times an authentication event takes place, as illustrated below.

Authentication Method	Convenience	Assurance
Use of mobile handset	Passive	Low
Account PIN entry	↓	↓
Account password entry		
Digital certificate authentication challenge	Disruptive	High

Figure 2 – Convenience and assurance in authentication methods

Highly assured authentication methods are clearly preferred when the value of the transaction or authorization is also high.

Authentication methods requiring more thought or interaction from the user are, in general, more disruptive but more assured. Highly assured authentication methods are clearly preferred when the value of the transaction or authorization is also high, as they aid in proving accountability should the need arise.

A well-designed authentication model will not disrupt the user without good reason or unless there is a need to raise the assurance level of the user's identity.

For example, if a network supports a digital certificate authentication challenge as its highest form of authentication—and a user has recently satisfied this as part of a high-value m-commerce transaction—there is little reason to require him to authenticate to a lower assurance authentication level for a less valuable transaction.

By forcing the user to stop and consider actions before they are carried out, disruptive authentication can protect the user, his or her finances, the network and other users from inappropriate or accidental access or agreement. A good security architecture will be able to invoke and apply the appropriate method.

Single Sign-On

One of the primary business goals of the CDF is to complete separation of the operator's users from its suppliers. For this reason, it is important that user identities always remain within the operator network. The authentication framework needs to support this and, if properly implemented, provides the user with a rich, single sign-on capability enabling access to all the products to which the user is entitled and at all required assurance levels. This means that a user who satisfies a digital certificate challenge whilst purchasing valuable goods at one mobile retail shop may not have to re-authenticate to purchase similar, or a lower value of, goods at another.

Regardless of how many retailers or content providers the user has interacted with using the same credentials, the operator must provide robust audit and accountability records for each transaction.

Managing Suppliers

Operators will use the CDF to deliver services and translate the content into appropriate formats suitable for end-user devices. It also provides a mechanism to control user access to the content. However, while these tasks are self-contained and provide value to the various parties, the real purpose behind a CDF is to abstract an operator's subscribers from the content suppliers. That is, to identify the user, the mobile device they are using, the levels of security required concomitant with the services they are using and the actual services they are using.

Without this, the mobile operator would decay into just another internet service provider or internet portal and wouldn't own its subscribers any more than Google™ owns its users. This is important because, unlike Google, mobile operators often enter into contractual commitments with a customer to supply them with mobile equipment amortized over 12 months or more—not to mention colossal network investment.

Common Services Gateway

Another part of the operator's architecture devoted to the task of abstracting its customers away from its suppliers is the Common Services Gateway (CSG). In its simplest form, the CSG should provide a set of standard interfaces into the services provided by the operator (See Figure 1). Some relevant examples include:

- > M-payment services
- > Audit and non-repudiation services
- > Data protection services.

The operator ... bears a significant burden of risk that must be mitigated with effective security practices and capabilities.

M-Payment Services

Convergent billing services enabling m-payment are a good example of operator-provided services and provide significant synergy between the involved parties. When users can purchase goods and services from third-parties—and pay for these with their pay-as-you-go minutes, credit cards or other pre and post-payment methods—everyone wins. The operator, however, bears a significant burden of risk that must be mitigated with effective security practices and capabilities.

To support the auditing of virtually any activity on the operator network, especially those involving customer payments, a robust audit logging service is required. Timely access to the logs and the assurance that they are preserved with high levels of integrity are imperative. A strategy to prevent log tampering and loss, whether accidentally or deliberately, is required.

In addition, since these logs will often contain subscriber-sensitive information, care must be taken to encrypt data when necessary. If a customer disputes a transaction it is important that the audit log details correspond with the transaction details to support or disprove (as the case may be) the customer's claim, hence the need for data encryption.

Further support is provided by a single, consistent, tamper-resistant, network-wide, high-availability time source and associated time-stamping service.

Data Protection Services

The operator or one of its suppliers often needs to maintain stored data on behalf of the subscriber. It may also need to archive data for a number of years to maintain compliance with local or regional data protection regulations. To facilitate this compliance, a service should exist to allow seamless and secure storage and retrieval of the information to the operator or to third-parties. While this is not a simple matter, a properly constructed architecture facilitates such capabilities.

Specific User Profiles

In today's mobile internet world, users expect to interact with organizations they already have relationships with, such as their bank or favorite retailers. In these cases, it is natural for the third parties to maintain their own relationships with the end-user. In fact, in the case of mobile banking, the operator must provide end-to-end encryption between the end-user and the bank itself.

In some cases, the operator will want to extend a view of its customer profiles to third-parties. This must be done within strict controls and always within the scope of subscriber agreements and all applicable laws and regulations. The infrastructure must provide the tools required to comply with and audit such transactions.

As spelt out earlier, subscribers must trust the operator. Part of this trust requires the operator to prevent the unauthorized collection or misuse of subscriber information. There is a raft of increasing regulations designed to ensure this discipline is maintained and not keeping within these boundaries can result in severe penalties. Even without these regulations, it is clearly in operators' best interests to prevent these practices as much as it is to protect their customer lists. Great care must be taken to achieve these goals, especially when there is also the desire to provide seamless, personalized content.

Security 'Baked' into the CSG

The CSG, like the CDF, is an integral part of the security infrastructure. While the CDF is responsible for access-controlling users, the CSG is responsible for access-controlling suppliers. In each case, the access control function must identify the calling party, and authorize (or not) each request. This can be accomplished by issuing identities to each supplier, which will accompany each request into the network. The access control function at

... a high capacity network link, when harnessed by an attacker, can wreak havoc on an operator by becoming a very effective means of launching ... attacks.

the CSG verifies the validity and integrity of the identity within each request and verifies that this particular supplier has access to the requested service. This needs to happen in real-time and in high volumes.

Attacks from the Supplier's Network

The operator must plan for its peak-traffic periods and this means that the architecture and third-party suppliers must also have the capacity to handle these peaks. This introduces a number of important security issues for the operator. First and foremost, it means that the security controls enforced at the CSG cannot unacceptably tax the performance of the system.

Content suppliers who are providing high-data throughput will more than likely utilize server farms to keep up with high demand and guard against failure. But these suppliers will also need to use high-capacity network links to the mobile communications operator. These two aspects are an essential requirement for a content delivery system capable of high capacity delivery.

High-capacity content suppliers will often utilize server farms to keep up with the demand and guard against failure. The suppliers will also use a high capacity network link to the operator. These assets are a requirement for a capable content delivery system, but when harnessed by an attacker can wreak havoc on an operator by becoming a very effective means of launching and sustaining distributed and/or denial of service attacks. Very careful consideration must be made, therefore, when connecting such networks.

It is an easy decision to simply cut network ties with the supplier on first sign of a security problem, but doing so will also sever any ongoing interaction with the subscribers and the associated revenue it generates. Containment of the security problem to those affected servers, and selectively disabling access to the operator network, is preferred as it preserves the revenue stream. A security architecture that proactively aids in the identification and isolation of problems is a real asset that can save the operator significant revenue.

Managing the Supplier Lifecycle

Once the operator controls the interfaces at both ends, it is fairly straightforward for it to manage the lifecycle of its suppliers. It will be able to establish which alliances will be useful by being able to determine which services are proving popular with end-users. It will also help the company determine the driving forces for cooperation. This helps the operator mitigate risks associated with suppliers and gives the operator a leveraged position when negotiating new supplier contracts.

Customers will be drawn to an operator as a result of the services on offer, but underpinning this dynamic is the need to provide a secure service in which the user can trust implicitly.

Conclusion

Operators that are able to maximize their understanding of customer information and seamlessly provision new products and services while maintaining an efficient network are well positioned to remain competitive despite rapid industry change. This is critical as e-products and services rapidly emerge and subscribers demand a network operator who will bring them to market quickly and cost effectively.

However, operators need to understand who their customers are and what their needs are too. If customer data is fragmented an operator's understanding of its customers will also be fractured, leading to sub-optimal quality of service and increasing the likelihood of customers churning to rival services. The operator's product and service delivery architecture should be developed with these imperatives in mind.

Customers will be drawn to an operator as a result of the services on offer, but underpinning this dynamic is the need to provide a secure service in which the user can trust implicitly. One of the key questions a user will ask is whether the mobile services are vulnerable to fraud and identity abuse. If an operator cannot reassure the customer, the service is doomed to failure from the outset. If the operator can reassure the customer the chances of success are significantly enhanced.

Information security 'baked' into the operator is an essential component that will not only enable an operator to provide all round security but also enable many of its key features such as the Content Delivery Framework and Common Services Gateway. These features not only underpin security management but also allow an operator to establish patterns of usage and popularity of particular services, thereby informing the operator's future strategies too.

Operators who realize this will quickly realize their goals and be ideally positioned to manage the future of m-commerce.

About Atos Origin

Atos Origin is an international information technology (IT) services company. Its business is turning client vision into results through the application of consulting, systems integration and managed operations. The company's annual revenues are more than EUR 5 billion and it employs 47,000 people in 50 countries. Atos Origin is the Worldwide Information Technology Partner for the Olympic Games and its clients include ABN AMRO, Akzo Nobel, Alstom, BNP Paribas, BP, Ericsson, EDF, Euronext, Fiat, France Telecom, ICI, ING, KPN, Lucent, Philips, Renault, Royal Bank of Scotland, Saudi Aramco, Schlumberger, Shell, Telecom Italia, UBS, UK Department for Work and Pensions, Unilever, Vivendi Universal and Vodafone. For more information, please visit the company's web site at www.atosorigin.com Atos Origin is quoted on the Paris Euronext Premier Marché and trades as Atos Origin, AtosEuronext, Atos Worldline, Atos KPMG Consulting and Atos Odyssee.