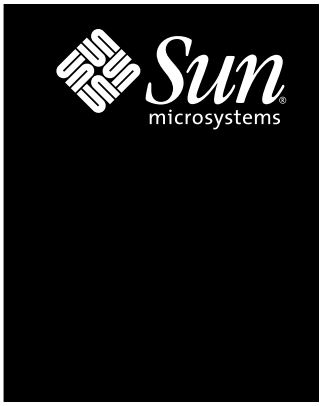
Leveraging Identity in Public-Access Wi-Fi Networks

A Technical White Paper
August 2004



Please
Recycle

Adobe PostScript

Table of Contents

Chapter 1
Introduction

The market for public-access Wi-Fi networks is poised for rapid growth, and telecommunication carriers, including telephone companies, cable operators, wireless carriers, and DSL providers, are well positioned to profit from this expanding market. Indeed, as the range of Wi-Fi-enabled devices broadens, so does the demand for Internet access anywhere, anytime. Not long ago, early adopters had to purchase and install their own wireless cards into their laptop computers; whereas today, Wi-Fi networking is a standard feature that customers have come to expect. Personal Digital Assistants (PDAs), MP3 players, digital cameras, and even cell phones are beginning to provide Wi-Fi networking capabilities — and as they do, they are likely to push the demand curve even more steeply.

As users of this rapidly-expanding set of devices demand greater access, Wi-Fi network operators of all sizes are rapidly expanding their coverage footprint by deploying large numbers of hotspots. As reported in the People's Daily Online ("Public Wireless Networks to Grow Fast over Next Five Years," July 11, 2003), Allied Business Intelligence (ABI) expects the 28,000 hotspots they counted worldwide to grow to 200,000 in only five years — an annual growth rate of more than 48 percent! ABI predicts the revenue these hotspots generate to reach USD $3.1 billion by the year 2008.

Such growth rates are reminiscent of the ISP market boom of the late 1990s — and also of some of the lessons that the boom taught ISPs. Rapid growth brought increased competition, making basic Internet service a commodity, and putting downward pressure on prices. In the public-access Wi-Fi market, early entrants can enjoy relatively high prices for basic network access, but over time an increasing number of hotspots is likely to foster competition that results in commodity pricing. Ultimately, there is little value in the network pipe itself — those offering the fastest, lowest-cost pipe will win, and some network operators will be acquired or lose ground to the competition.

The Value of Innovative Services

Wireless carriers which offer innovative business applications to their customers will likely benefit, rather than suffer, from the commodity pricing with which other carriers will struggle. This is because their revenue streams can be complemented with income generated by features that customers are willing to pay for, by services provided to business partners and delivered over their networks, and by productivity applications that help enterprises increase the productivity of their mobile workforces. Value-added services that add to a network operator's top-line revenue aren't limited to e-mail and calendaring; they will be truly innovative features that leverage the mobile nature of their customers. Imagine:

- Fast food restaurants rewarding their customers through affiliate marketing campaigns. Once a customer accumulates sufficient points, they can download a free music selection from a partner site onto their wireless MP3

player right in the restaurant. Both businesses benefit, and the goods delivered are all virtual, requiring no packaging, distribution, nor inventory control, as the trinkets of today require.

- Enterprises supporting their mobile workforces with applications available through public-access Wi-Fi networks. Real-estate agents, for example, need mobile access to internal, local-office information, they need to use third-party sales automation tools, and they need access to their multiple-listing services. All of these can be supported with single sign-on through a personalized portal.
- Cell phone users roaming freely between cellular and Wi-Fi service areas. Enterprises can reduce phone costs significantly by equipping their workforce with Wi-Fi-enabled cell phones and installing Voice-over-Wireless-LAN (VoWLAN) technology on their campuses.
- Location-based services guiding wireless device users to special promotions in the local store, while making it easy for them to visit the company Web site to view and order items not in stock.
- Customized portals offering personalized services through which users can access services like e-mail, calendar, address book, portfolio, travel information, local weather, and single sign-on to a range of cooperating sites. Carriers can provide portals for use by laptop-based Web browsers and also by thousands of different wireless devices including cell phones and PDAs.
- Digital photo-printing kiosks accepting images from Wi-Fi-enabled cameras to print, post to the Web, or archive, depending on the services allowed to each family member.

The key technology driving all of these scenarios is network identity management integrated into the network operator's Operations Support Systems (OSS). Network identity management allows all subscriber information including usernames, passwords, credit card numbers, addresses, application preferences, and other personal information to be securely managed at a central location. It supports Single Sign-On (SSO) for Web sites, allowing affinity program customers, employees, and portal users to log in once and then use the range of services they need from a variety of sites without having to log in again. Good network identity services give customers the power to decide how much of their personal information may be shared with which sites.

Integrated Network Identity from Sun and Pronto

It should come as no surprise that two leaders in public-access Wi-Fi technology — Pronto Networks and Sun Microsystems — have already integrated network identity services into public-access Wi-Fi network management software to create the platform that operators will need to put themselves ahead of the pack today, and to maintain that position in the future. Pronto Networks offers a complete, integrated OSS for providing Wi-Fi services with key Application User Interfaces (APIs) that can be integrated with legacy systems already used by telecommunication carriers. Pronto Networks has integrated their carrier-grade Wi-Fi service management platform with Sun Java™ System Access Manager and Sun Java System Portal Server to provide the foundation on which carriers can support value-added services that can leverage network identity. Sun Java System Access Manager helps carriers improve user experience by making it easy for customers to log in at Pronto Networks-powered hotspots and those with which they have roaming agreements. Once logged in, customers can take advantage of identity-related functions supported by their carriers. Sun Java System Portal Server delivers a platform that carriers can leverage to deliver a personalized user experience to customers, including content aggregated from a variety of providers, and services including e-mail, calendaring, and address book functions. The combination of Pronto Network's Wi-Fi experience with Sun's best-of-breed identity management and portal software gives forward-looking carriers the tools they need to stay ahead of the competition.

This white paper details several innovative business applications that carriers can deploy using integrated OSS and identity services, it describes the synergy between both company's software products, and it shows exactly how identity management can be used to support value-added services.

Chapter 2

Innovative Business Applications

The combination of network identity management with Wi-Fi service management provides a foundation on which network operators can build innovative business applications that will be key to their long-term success. The way in which the Pronto OSS integrates services from Sun Java System Access Manager results in a highly scalable, flexible platform that network operators can use to deliver their own value-added services. It also provides an underlying mechanism through which operators can act as 'identity providers,' supporting innovative services through collaboration with other business entities.

For network operators looking to provide a range of innovative business applications, three identity management features are essential:

- *Single Sign-On* improves user experience by allowing users to authenticate to the operator's network once, and for them to be logged into operator's, partner, and affiliate sites automatically, as long as their Wi-Fi connection is maintained. SSO can be used to authenticate subscribers into personalized portals that are delivered as a start page. Likewise, SSO can be used to authenticate the subscriber to sites outside of the operator's domain.
- *Access Management Services* help make the delivery of business information secure. While RADIUS is the standard used to authenticate users to *hotspots*, network identity authenticates users to *applications*. When business entities partner with network operators to provide secure remote access to their employees, network operators using Sun Java System Access Manager have the ability to let them determine what information and applications each employee can access, based on their role in the organization.
- *Federated Identity Management* allows network operators to form *circles of trust* where partners and affiliates can have access to user and session information — all under the control of the subscribers themselves. When federated identity management is implemented with open standards, like Security Assertion Markup Language (SAML) from the Liberty Alliance, network operators can create new revenue opportunities through affinity relationships with business partners and their subscribers.

Wireless carriers with integrated OSS and identity management systems have a range of choices in how they increase their revenues through innovative applications. They can implement some themselves, for example using Sun Java System Portal Server to provide a personalized start page to their subscribers. They can implement them on behalf of their business customers, for example providing services to support a mobile workforce. And they can implement some of them simply by acting as an identity service provider, supporting services that allow multiple business partners to join forces in affinity programs.

The range of potential applications that network operators can deliver is limited only by the imagination. The remainder of this chapter describes just a few example services that could use the potent combination of Pronto OSS and Sun Java System Access Manager.

Affiliate Marketing

Network operators that support a federated identity framework can support affinity relationships between multiple business partners. Consider how a fast-food restaurant could partner with an online music store to boost business for each enterprise, all while increasing use of the operator's services (Figure 1):

- A customer buys a meal and receives a code to enter on a wireless device to accumulate points.
- The customer logs in to the restaurant's Wi-Fi network using a wireless MP3 player, audio-enabled PDA, or even a laptop.
- The location-specific login screen gives the customer a link to the fast food restaurant's site. Following the link takes the customer to a Web application that accepts their code and adds points to their frequent-visitor club account. The customer is already logged in through the federated identity framework.
- Once the customer accumulates enough points, they can visit the partner's online music store to redeem them. The customer, who is already logged in through the network operator's single sign-on mechanism, can easily make download a selection, perhaps making an additional purchase at the same time.

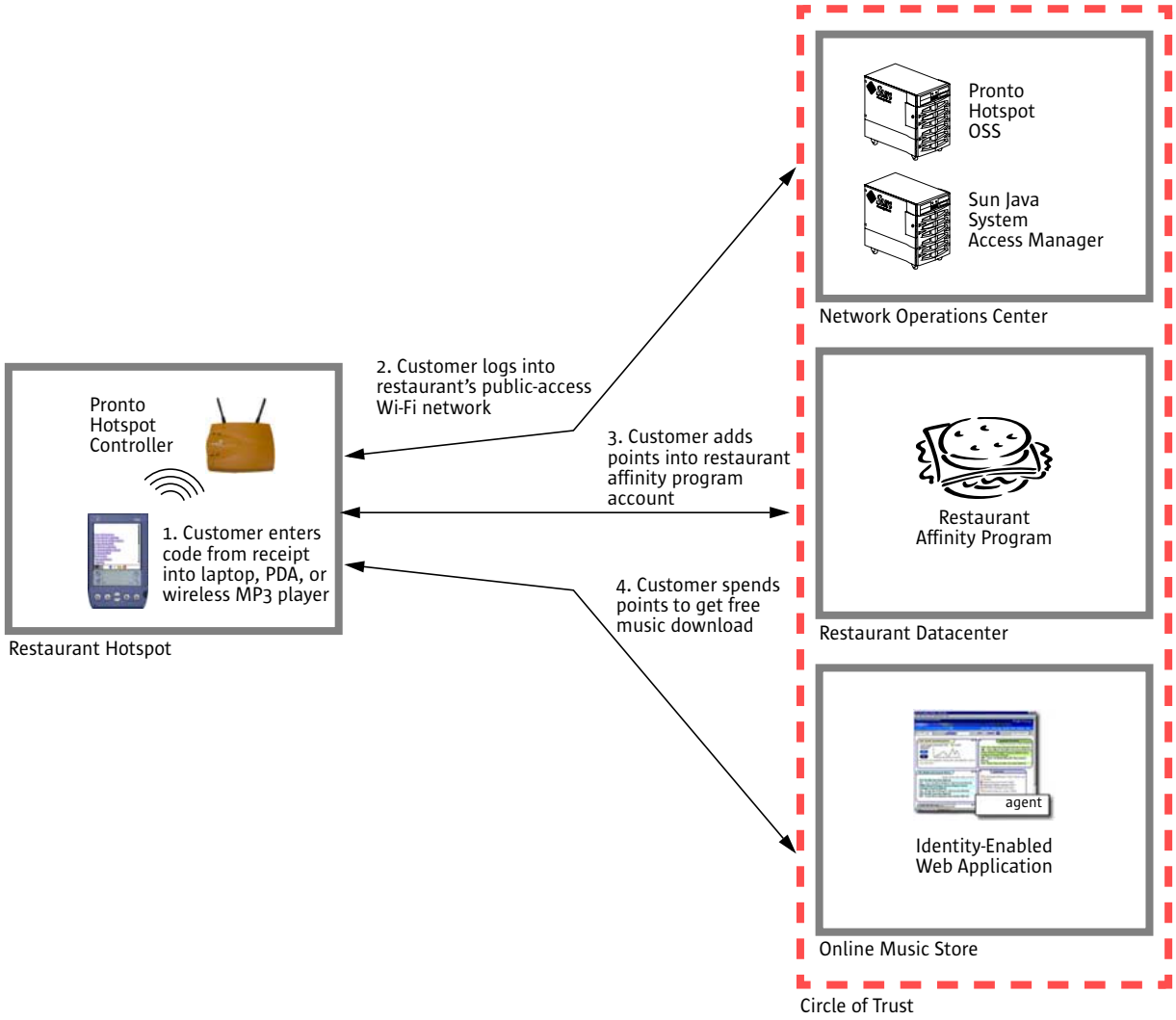


Figure 1. An affiliate marketing scenario allows restaurant visitors to accumulate points that can be redeemed for free music downloads.

This scenario not only helps to enhance both the restaurant and music store brands, and the federated network identity framework can also help to increase the revenue from both vendors to the network operator. The affiliate marketing program increases use of its network, potentially attracting more subscribers. And it embeds the network operator more fully into the restaurant venue, helping to expand the operator's footprint.

Voice-Over-Wireless LAN

A new breed of mobile phone is gaining in popularity — those with both cellular and Wi-Fi capabilities. These phones enable a business to connect employee calls through their existing Voice-over-IP networks while staff are on premises, while using cellular connections when away. This model can help companies reduce costs from the model of using cellular technology 100 percent of the time, but the real wins will come when the general public uses Wi-Fi-enabled phones virtually anywhere, in downtown hotzones, at home, and in specific venues — without even knowing when they're on a Wi-Fi versus a cellular network.

But who would use a phone that requires the user to log in every time they move to a new location? Using an identity-enabled OSS, network operators can provide single sign-on and a consistent user experience when customers are in their home carrier's coverage area, when they roam into a different operators' coverage area, and even if when foreign operator is not identity-enabled.

When network operators make it easy for customers to use technologies like Voice-Over-Wireless LAN (VoWLAN) through single sign-on and simplified roaming, they help create the critical mass of Wi-Fi phone users that will make the market boom. And once the market grows, the network operator that makes life the easiest will carry more of the VoWLAN traffic — and garner more of the revenue — than the competition.

Integrated Voice/Data Services

Carriers acting as identity providers can use Sun Java System Access Manager to support both identity and location-based services on voice, data, and video networks. Indeed, session management is a device and access network-agnostic service that can be used to support devices including laptops, PDAs, cell phones, and even set-top boxes.

Network operators can integrate identity services into telephone networks using the JAIN™ SIP API Specification. They can provide Session Initiation Protocol (SIP) profiles to called parties based on the caller's identity. Call centers, for example, can use a SIP profile to bring up a customer's account information while their call is answered. Vendors can use location information to help customers locate nearby services.

The ability of Sun Java System Access Manager to store application preference and profile information helps network operators wishing to provide subscriber and location-specific services. For example, a travelling subscriber might use a service to set up a wake-up call that also delivers the day's weather prediction for a specific locale. When integrated into e-mail and calendaring services, network operators can page customers on their wireless devices when a meeting is re-scheduled, for example.

Enterprise Managed Service Delivery

It's not difficult for organizations with a mobile workforce to see the value of providing managed services that help their employees do their job, whether at the office or on the road. Consider how an identity-enabled network operator can provide a managed service to a real-estate company, where agents work both in the office and all over town (Figure 2).

In the office, employees that log into the company's private Wi-Fi network are presented with a portal as their start page. The portal gives them access to internal applications such as e-mail and calendaring, and external, private ones like a multiple-listing service and a third-party sales force automation tool. When each of the applica-

tions participate in an identity-based circle of trust, employees can use the applications they need freely, without having to log into each one separately.

On the road, if a customer shows interest in a different kind of property, the agent can pull into the nearest hotspot, log in, and have immediate access to the same applications as in the office. The agent can accommodate customer needs and show new properties with only a brief detour to get new listings.

Whereas the affiliate marketing example illustrated a circle of trust involving a set of business partners, this example illustrates a circle of trust that includes internal, enterprise applications and extends outward to include external, private applications contracted for by the real estate firm. The identity-enabled network operator supports a consistent user experience, secure access to private applications, and ease of use through single sign-on. With its identity-enabled OSS, the network operator is able to grow its customer base by broadening into the enterprise environment.

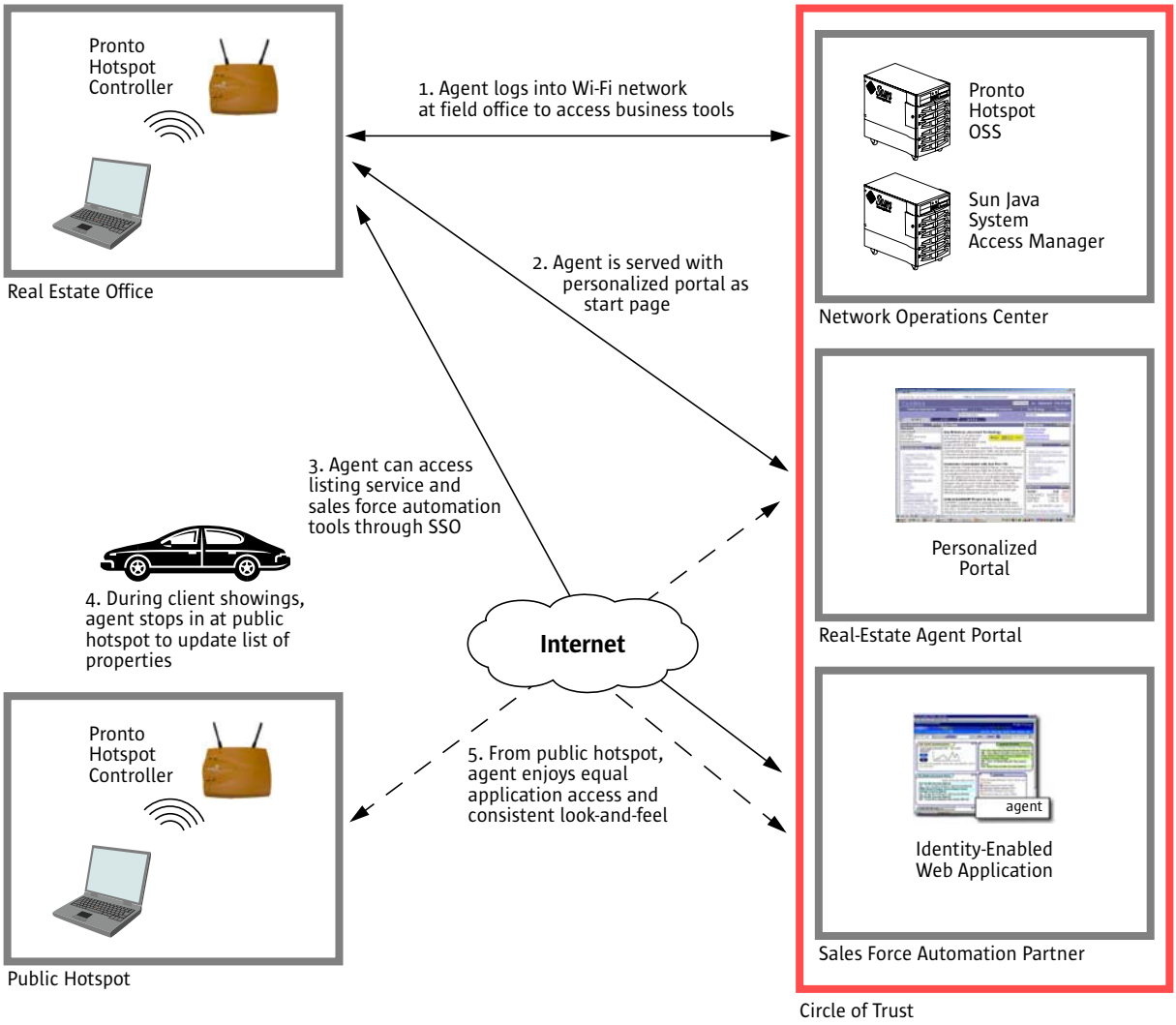


Figure 2. An enterprise managed service delivery extends a circle of trust into a corporate environment, while encompassing external, private applications.

Digital Photo Printing Kiosk

Wireless networking capabilities already can be found in high-end digital cameras, and it's likely only a matter of time until Wi-Fi and Bluetooth-enabled cameras become commonplace — opening up yet another market for wireless carriers. Consider a photo printing kiosk that offers prints and enlargements, and can post images to the Web on behalf of customers. Now consider the network operator that acts as an identity service provider, extending a circle of trust to the company operating the photo printing kiosks.

Once authenticated, the customer's photo printing preferences are available from the network operator's identity framework, and charges for prints can be added to customer's Wi-Fi service bill. Using Sun Java System Access Manager's delegated administration capabilities, customers can be allowed to set up sub-accounts, for example allowing a child to make a certain number or a certain dollar value of prints — without having to entrust them with keeping credit card numbers safe.

When a network operator acts as an identity provider, customers can set preferences and account limits through the network operator's identity framework. The greater the number of services tied into the circle of trust, the greater the affinity customers will have to that particular carrier. Likewise, as circles of trust are extended to a greater number of physical locations — such as photo printing kiosks — the network operator's brand gets extended as well.

Chapter 3

Enabling Technology from Sun and Pronto

Integrating identity and portal services into a carrier-grade OSS environment can help network operators get ahead of the competition by creating an arena in which they can offer an array of innovative business services such as those discussed in the previous chapter. The combination of technologies offered by Sun and Pronto can help network operators sell innovative services to existing customers, attract more customers through superior ease of use, augment both footprint and customer base by offering services to enterprise customers, and foster lucrative business partnerships with other companies recognizing the benefits that a federated identity framework can provide.

Relationship Between Products

When three key components from these two vendors are integrated, the following relationship exists between the Pronto OSS, Sun Java System Access Manager, and Sun Java System Portal Server (Figure 3):

- The Pronto OSS is built from the ground up to interface with a variety of external authentication services, for example: RADIUS and WISPr authentication to aggregators and clearinghouses for roaming users; SMPP for authentication through cellular wireless carriers; and credit card clearinghouses for on-the-spot payments. For users local to the network operator itself, the Pronto OSS can be configured to use standard LDAP or SQL databases — or it can be configured to use Sun Java System Access Manager through its custom APIs.
- Sun Java System Identity Server acts as the central repository for user information including accounts and passwords, and also for preferences and personal information that can be shared among partners (with users' permission). Once configured as the central user repository, it can support single sign-on and circles of trust among applications hosted within the network operator itself, among network operators (including support for roaming), among affiliated business partners, and even into enterprise environments.
- Integrating Sun Java System Portal Server into this configuration provides an example of how both products can be used to support a valuable service to customers. When a subscriber provides a valid username and password to the login page, the Pronto OSS authenticates the subscriber using Sun Java System Access Manager. Once the subscriber is authenticated and session information set up, the Pronto OSS responds to the subscriber with a start page, which could be a URL directing the browser to a personalized portal for that subscriber. The subscriber's preferences, stored by Access Manager, are used by Portal Server to create a custom start page, and the subscriber is automatically logged in thanks to the single sign-on relationship between applications within the network operator.

This describes the high-level relationships between products. The products contributing to this synergy are described in the following sections.

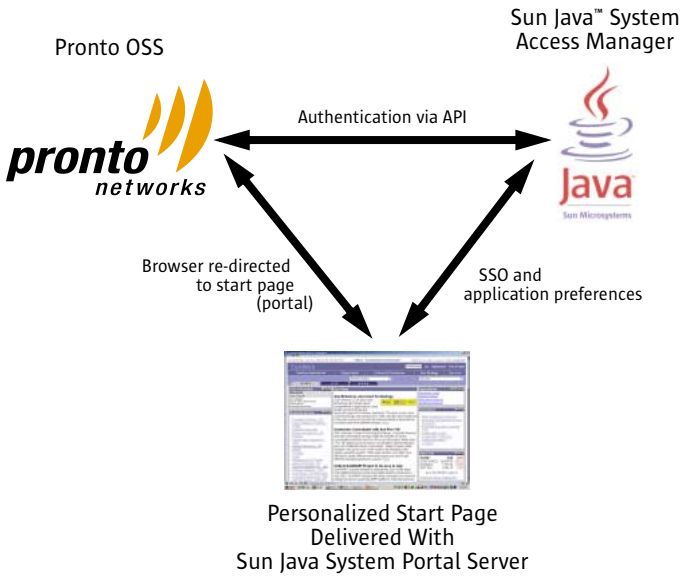


Figure 3. The Pronto OSS and Sun Java System Access Manager work together to support innovative applications, such as this personalized start page delivered with Sun Java System Portal Server.

Pronto OSS

The Pronto OSS is a carrier-grade operations and business support system for large-scale, public-access Wi-Fi networks. An integrated, end-to-end system, it can help telecommunication carriers get their networks up and running in short order, helping to reduce time to market while minimizing ongoing operational costs. As the foundation of any carrier's operations, it provides a flexible platform for carriers that wish to deploy innovative business applications. Pronto OSS includes modular, feature-rich components for:

- *Service creation, activation, and maintenance of hotspot locations*, making it easy to define a flexible range of service plans and then deploy and remotely manage the hotspots that support them. Service providers minimize installation costs through the self-provisioning capabilities of their Pronto Hotspot Controller™ devices.
- *Network policy implementation and monitoring*, including Quality-of-Service (QoS) support, monitoring capabilities, and easy integration with third-party network management system products.
- *Authentication, Authorization, and Accounting (AAA),* along with custom authentication realms, the ability to support multiple network operators, and the ability to integrate with Sun Java System Access Manager.
- *Roaming clearinghouse support for network partners*, including inter-Wireless ISP (WISP) roaming, integrated billing, clearing, and settlement, and built-in support for iPass, GRIC, and Boingo smart-client software.
- *Customer care and billing management*, including customer self-care and self-provisioning, and the ability to define numerous service plans, including pre-paid and post-paid options.
- *Payment processing and collection*, including configurable billing formats, and native integration to third-party billing and Customer Relationship Management (CRM) systems.

Multi-Platform Solution

Pronto OSS is a multi-platform solution that runs on the rock-solid Solaris™ Operating System, allowing it to run on Sun's scalable UltraSPARC® processor-based Sun Fire™ server products, and also on Sun's NEBS-compliant Netra™

servers that are built for the demanding environmental conditions of telecommunication carriers' central office facilities. Pronto OSS also runs on the Linux operating system, allowing it to leverage Sun's state-of-the-art rack-mount x86-architecture servers.

Multi-Vendor Solution

Pronto OSS manages deployment and operations using Pronto Hotspot Controller devices, and it provides a cost-effective access service gateway that supports third-party access points including many from Proxim, Cisco, Colubris, and Gemtek Systems.

Ready for Telecommunication Carriers

Pronto designed its OSS product leveraging the Java™ 2 Platform, Enterprise Edition (J2EE™) specification, providing Web services interfaces that can support secure, robust, and interoperable business applications. The platform provides the ability to integrate with third-party billing and CRM systems. Pronto OSS provides a set of APIs for custom data integration to and from external applications. Integration to certain services is readily available, such as e-mail integration with Critical Path. These options simplify the process of integrating Wi-Fi service management capabilities into telecommunication carriers' existing IT infrastructure, helping to reduce time to market and contain costs.

Sun Java System Access Manager

Sun Java System Access Manager provides a security foundation that allows network operators to manage access to applications hosted within its organization, among multiple business partners, and even in enterprise environments. It provides open standards-based authentication and policy-based authorization with a single, unified framework. When integrated with Pronto OSS software, it becomes the central repository for subscriber information, supporting access to both applications and networks, including roaming to foreign Wi-Fi networks. Features of key importance to network operators include:

- *Single sign-on* that improves user experience by enabling subscribers to use their identity established at network login time to access multiple resources, applications, platforms, and Internet domains. SSO forms the foundation on which network operators can support affiliate marketing programs.
- *Federated identity support* through Liberty Alliance Phase 2 and Security Assertion Markup Language (SAML) 1.1 specification compliance. These protocols enable authentication and authorization across federated business networks, providing increased revenue opportunities by supporting trusted partnerships — while helping to reduce costs with increased integration efficiency.
- *Session management* that maintains session state for subscribers that can be accessed by any of the applications for which SSO and federated identity are supported.
- *Delegated authority* can be used to set up hierarchies that, for example, can be used to allow a family subscriber to set up sub-accounts — with unique application preferences and spending limits — for each family member.
- *J2EE architecture and comprehensive APIs* are used to build an open standards-based system that helps carriers implement high levels of integration and customization. The use of the J2EE specification allows developers — such as those creating innovative business applications — to extend their existing Java™ technology skills, helping to reduce cost and time to market.
- *Enterprise-class scalability and reliability* helps Access Manager grow with the speed of a network operator's business, while providing availability levels appropriate for telecommunication carriers. Sun Java System Access Manager can be deployed in ways that help eliminate single points of failure, for example through the use of multiple load-balanced policy servers, policy agents, and directory instances that provide high availability and failover capabilities.

- *Real-time audit* provides up-to-the-minute auditing of all authentication attempts, authorizations, and changes, delivering improved security with instant auditing of critical access-related information.

Sun Java System Portal Server

The perfect first application for network operators to deploy using their identity-enabled OSS is Sun Java System Portal Server, the industry's first identity-enabled portal server solution. It delivers personalized content, applications, and services to subscribers by dynamically aggregating information based on the subscriber's role. Once logged into the portal, subscribers can simply and easily customize their portal's content, layout, and interface to fit their needs. Sun Java System Portal Server can be augmented to provide secure remote access to enterprise applications, services, and data using Sun Java System Portal Server, Secure Remote Access. It also can be extended to tailor its content for optimum usability from thousands of cellular mobile devices using Sun Java System Portal Server, Mobile Access.

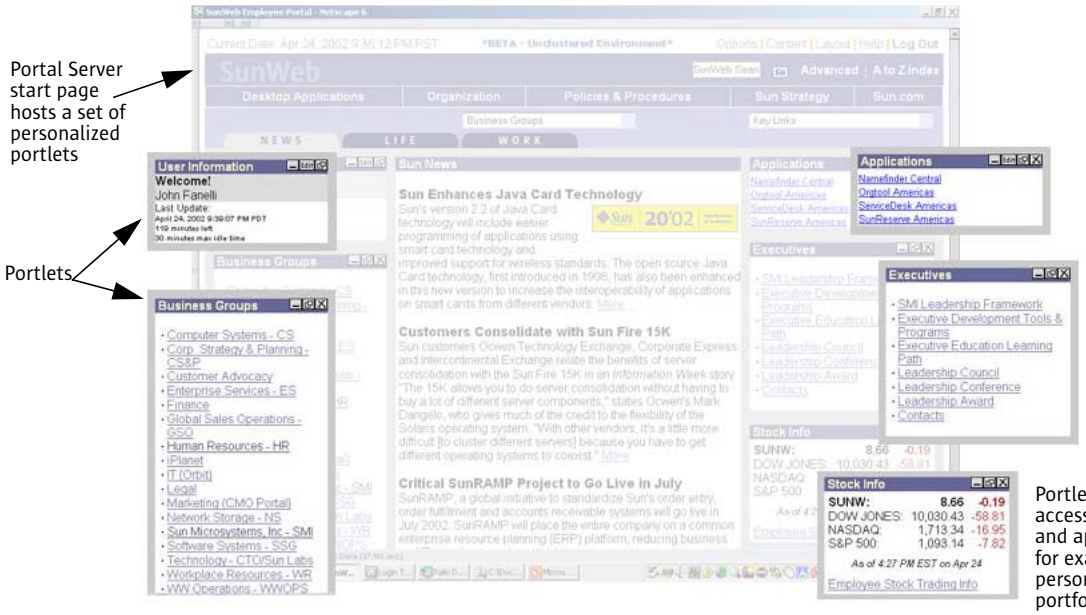


Figure 4. Sun Java System Portal Server aggregates and presents information and services from a variety of sources through a set of portlets that subscribers can arrange and personalize.

Sun Java System Portal Server aggregates content from a variety of sources and presents each source through its own *portlet* (Figure 4). Portal Server provides an easily-extended framework with a large number of portlets included with the product itself, with a significant number available from Independent Software Vendors (ISVs) as well. For those wishing to develop custom portlets, it's as easy as writing Java software that conforms to the open-standard Java Portlet Specification.

Sun Java System Portal Server is capable of presenting a rich variety of information and applications, including e-mail, calendaring, address book, syndicated news feeds, Rich Site Summaries (RSS) through RDF technology, PC desktop and server applications, and personal information like stock portfolios. When used to provide secure remote access to enterprise applications, those applications and other internal Web sites can be accessed through the layer of SSL encryption that the portal provides.

Chapter 4

Leveraging Identity Services

After acquiring customers, the biggest challenge faced by telecommunication carriers today is keeping their subscribers. Telecommunication carriers work hard to increase customer loyalty by creating multiple ways to tie their customers to them. They create bundles of services, for example terrestrial and cellular telephony packages, and personalized experiences that help keep their subscribers from straying to the competition.

The public-access Wi-Fi networking market is no exception. Once they acquire customers, network operators need to work hard to retain them, and the combination of single sign-on and federated identity gives them the leverage they need to deliver:

- *Innovative business applications* that help network operators stay ahead of the competition,
- *Single sign-on experience* whether at home, at work, or while traveling, and
- *Personalized user experience* that follows subscribers even when they roam.

A personalized experience that remains constant even when subscribers roam to other carriers has significant value in counteracting the opportunities that roaming partners have to market their services to a network operator's customers while they roam. The ease of providing such an experience, using an identity-enabled OSS, provides a compelling argument for building a Wi-Fi service management architecture with integrated identity management.

This chapter describes the technical detail of how identity management is integrated into the Pronto OSS from two points of view: how a user logs into their local, identity-enabled network operator, and how login works for a roaming subscriber logging into a non identity-enabled network operator's hotspot. It illustrates how identity management can support SSO at the local network operator and circles of trust with affiliates.

Logging In at The Local Network Operator

The simplest way to illustrate how identity management integrates with the Pronto OSS is to follow the subscriber login sequence illustrated in Figure 5:

1. The Pronto Hotspot Controller displays a splash page asking the subscriber to enter a username and password.
2. The username/password is delivered via a form post to the Pronto Hotspot Controller device, which uses the information to form a RADIUS query to the Pronto OSS.
3. The Pronto OSS receives the RADIUS request and asks Sun Java System Access Manager to validate the request using the APIs provided for this purpose.

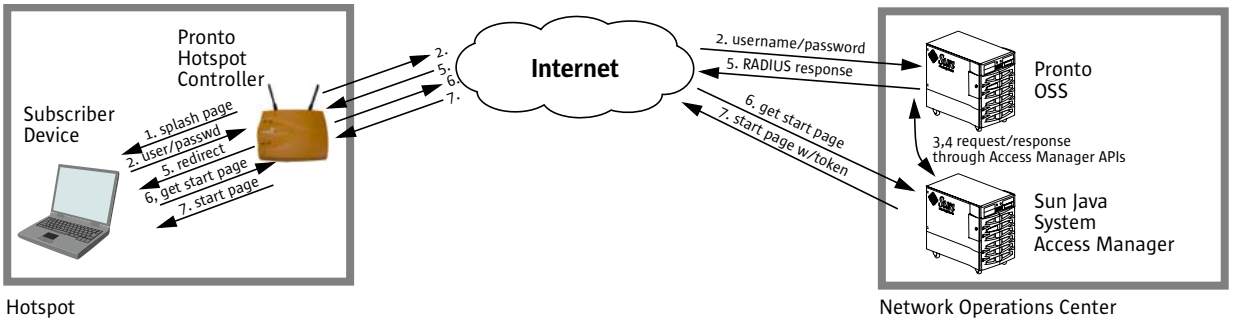


Figure 5. The subscriber login sequence for home operators uses both identity-enabled and RADIUS authentication.

4. Sun Java System Access Manager validates the username and password, and creates an *identity token*. The identity token is a random number that identifies the session that the subscriber has initiated. The identity token will later be delivered to the subscriber's browser in the form of a cookie that identifies the session. Access Manager tells the Pronto OSS that the username/password pair is valid.
5. The Pronto OSS provides a RADIUS response to the hotspot controller using the WISPr specifications to designate a URL to which the subscriber's browser should be redirected. The hotspot controller opens up Internet access for the subscriber, and it passes a page containing the HTML redirect to the subscriber's browser.
6. The subscriber's browser automatically requests a start page from Sun Java System Access Manager.
7. Sun Java System Access Manager receives the request for the start page, identifies the subscriber as having a valid session, and responds with a page that includes the identity token in the form of a cookie. This token can be used to support single sign-on to other identity-enabled applications. Access Manager could be configured, for example, to deliver a start page that is actually a redirect to a portal provided by Sun Java System Portal Server. When the portal server receives the subscriber's request as a result of the redirect, it also receives the session token, automatically logging in the subscriber, providing a personalized portal.

The two-step login to both the Pronto OSS and Access Manager may seem on the surface to be overly complex. Consider, however, that this technique allows low-cost, third-party hotspots to be used in identity-enabled network operators by virtue of the fact that no identity-related functions must be implemented in them. Standard RADIUS protocols are used between the hotspot and the Pronto OSS. This approach also helps to support roaming to non identity-enabled network operators, as described in the following section.

Roaming at a Non Identity-Enabled Network Operator

Logging into a non identity-enabled network operator, a roaming subscriber is issued an identity token so that they may also reap the benefits of single sign-on and federated identity services. Because the procedure uses standard RADIUS protocols, identity-enabled network operators can give their customers the same experience even through roaming partners (Figure 6):

1. The remote network operator's access point presents a splash page to the subscriber. Depending on the implementation, the page may be served from a Web server on the access point itself, from a separate access controller, or from the operator's OSS. The following steps assume that the access point includes an authentication mechanism.

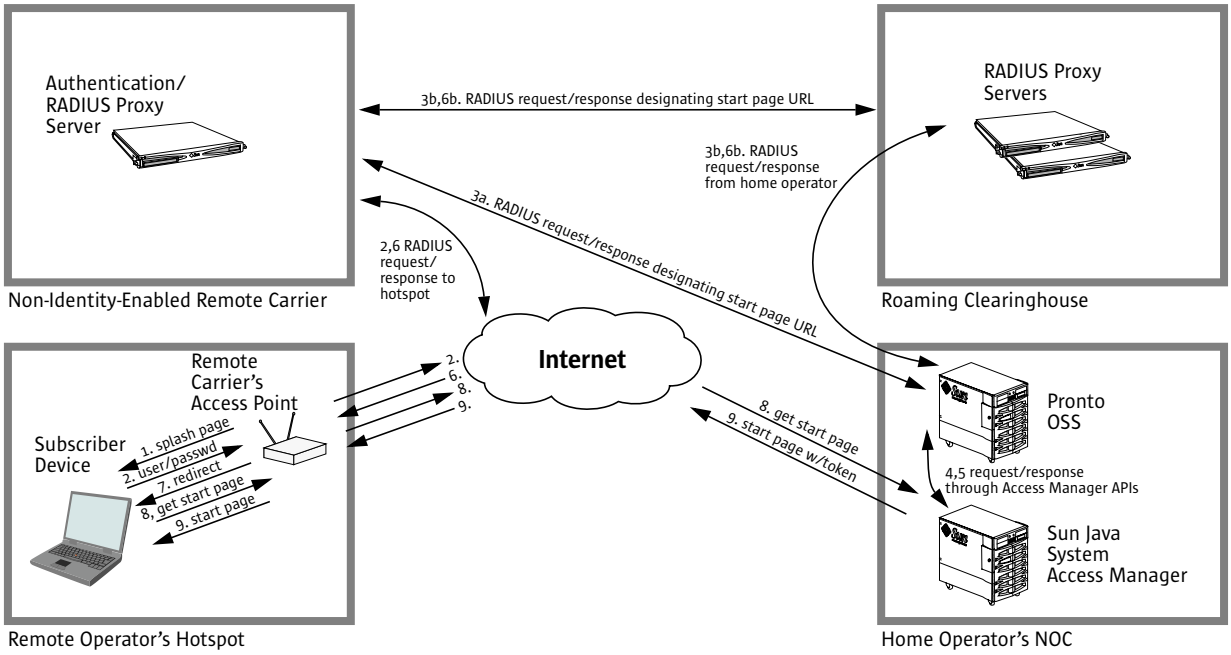


Figure 6. The subscriber login sequence through a remote network operator (roaming) uses RADIUS authentication directly to the home network operator or through a clearinghouse.

2. The subscriber enters a username and password, and posts the form to the access point by pressing a "submit" button. The access point translates the username/password into a RADIUS request that it passes up to the remote operator's authentication server.
3. The remote network operator's authentication server recognizes the username/password as non-local, and acts as a RADIUS proxy, forwarding on the request to one of two authentication sources:
   a. If the subscriber is roaming from a known roaming partner, the RADIUS request is passed directly on to the partner's RADIUS server. In this case, it's the home operator's identity-enabled OSS.
   b. If the subscriber is not from a known partner, the RADIUS request may be passed to a roaming clearinghouse, which in turn contacts the home operator's authentication server.
4. Regardless of how the authentication request was passed to the home operator's identity-enabled OSS, the Pronto OSS contacts Sun Java System Access Manager through its APIs to validate the username/password pair.
5. The Sun Java System Access Manager establishes a session and creates an identity token that will later be passed to the client. It gives the Pronto OSS a positive response.
6. The Pronto OSS fashions a RADIUS response that designates a start page for the user, one that points to the Access Manager itself. The RADIUS response is returned through one of two routes:
   a. If the partner is known, the Pronto OSS responds to the remote network operator's RADIUS proxy, which in turn passes the response to the access point.
   b. If the request was sent through a clearinghouse, it takes a corresponding route back to the access point.
7. The access point opens up its firewall and passes the designated start page URL to the wireless client with a page containing an HTML redirect.
8. The subscriber's browser automatically requests a start page from Sun Java System Access Manager.

9. Sun Java System Access Manager receives the request for the start page, identifies the subscriber as having a valid session, and responds with a start page that includes the identity token in the form of a cookie. This token can be used to support single sign-on to other identity-enabled applications. Access Manager could be configured, for example, to deliver a start page that is actually a redirect to a portal provided by Sun Java System Portal Server. When the portal server receives the subscriber's request as a result of the redirect, it receives the session token, and automatically logs in the subscriber, providing a personalized portal.

This process allows the home network operator to 'own' the subscriber by delivering the same familiar experience whether their subscriber is in their home area, or roaming through a partner's coverage area.

Implementing Circles of Trust

Once a subscriber has logged into the identity-enabled network operator, the network operator's Access Manager maintains session information associated with the identity token generated at login time. This token can be used to support single sign-on across applications hosted by the network operator itself, and by applications hosted by business partners outside of the network operator's Internet domain. All use of the token must be validated by the network operator's Access Manager, making it the central authority for information regarding a user session. It is also the central repository for personal information and application preferences that the user wishes to share across a circle of trust. This "opt in" model gives subscribers confidence that they have control over how their information is to be used, increasing the likelihood that they participate in, and benefit from, the circles of trust that the network operator supports.

Web applications, both in and outside of the network operator, host an agent which serves as a gatekeeper for the application. It examines credentials from the subscriber and determines whether access is to be granted, and what policies and user preferences apply. Personal information is encrypted by the Access Manager and transmitted securely to the agent guarding the Web application using Liberty Alliance protocols.

The login sequence for a Web application that is out of the network operator's domain proceeds as illustrated in Figure 7, assuming that cookies are used to contain the identity token in this case:

1. The subscriber attempts to access the Web application and the browser's request is intercepted by the application's agent. The agent does not receive an identity token with the request and denies the access. Note that the subscriber's session is valid, but it is not yet recognized by the agent because the agent cannot see the token because it is issued in a different domain and therefore is not accessible.
2. The agent, however, is configured for Cross-Domain Single Sign-On (CDSSO), and responds to the request with a "please wait" page that re-directs the subscriber's browser to the network operator's Access Manager. The Web page containing the redirect contains a form post request along with Liberty Alliance parameters which identify exactly what page was requested.
3. The subscriber's browser automatically posts this form data to the network operator's Sun Java System Access Manager. Because the post is made to the Access Manager that originally issued the identity token, the token is presented to the Access Manager along with the form data, allowing it to correlate the session with the desired Web application.
4. The Access Manager responds with a page that redirects the subscriber's browser back to the original Web application, this time the page includes the Liberty POST Profile containing SSO session information.
5. The form is automatically posted to the Web application, presenting the encrypted credentials to the agent, which validates them and grants access to the application.
6. The Web application responds to the subscriber with its own content, including a session token that is relevant to the domain in which the application is hosted.

7. Once the agent has credentials identifying the subscriber and the session, the agent can access policy information from the Access Manager, and it can register interest in the session and 'listen' for any changes that would require the agent to automatically terminate the session, for example when the subscriber logs out from the network operator.

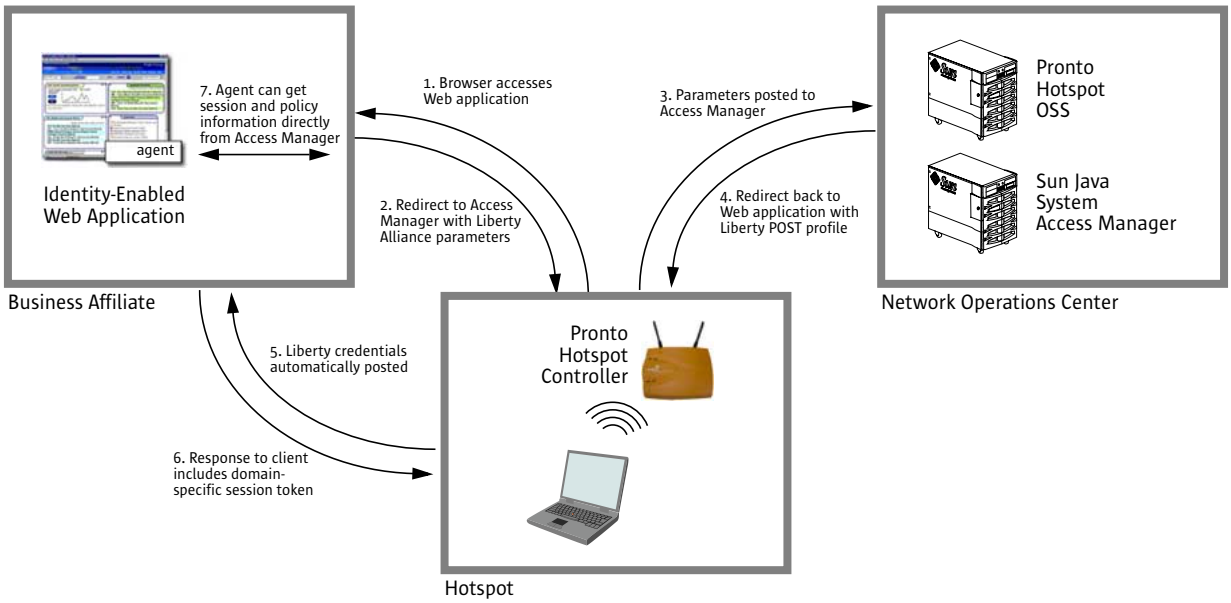


Figure 7. Cross-domain single sign-on securely exchanges subscriber credentials via Liberty Alliance protocols.

Chapter 5
Conclusion

As the market for public-access wireless networking grows and matures, the winners will not be those providing network access and bandwidth alone. The value to customers is not in the network itself, but in the innovative services that add real value to the experience. Personalized portals that give a consistent user experience at home, at the office, and at venues served by hotspots worldwide; affiliate marketing campaigns that increase the value to all participants while increasing the use of wireless networks; enterprise managed services that increase employee productivity and help put their companies on the leading edge; seamless Voice-over-Wireless LAN roaming that makes it easy to use public-access Wi-Fi networks for telephony — all of these are examples of the kinds of services that can help network operators pull ahead of the competition today and stay ahead in the future.

The enabling technology for many of these innovative business applications is the integration of network identity management with the operations support systems that keep public-access Wi-Fi networks up and running — whether based on 802.11, 802.16 (WiMAX), or future technologies. Whether a network operator chooses to offer value-added services themselves, or to use network identity to support circles of trust used by their business partners, having this technology in place can be a key asset for building interesting, innovative, and profitable services.

The synergy between Sun Microsystems and Pronto Networks makes the choice of which vendors to partner with an easy one. Both Sun and Pronto have the products and the experience that network operators need to implement this critical technology into new and existing operations support systems. They have gained this experience not only from having integrated identity management with OSS software; they have gained experience from actually implementing their products in real-world environments.

Pronto Network, with its Pronto OSS, can help network operators get up and running quickly with its out-of-the box functionality and APIs for integration with existing systems common to telecommunication carriers. Features like provisioning, authentication, accounting, administration, customer relationship management, billing, network management, service plan creation, and roaming provide the core services that all network operators need in an easy-to-deploy package. Sun Microsystems, with Sun Java System Access Manager and Sun Java System Portal Server, has the software that meshes easily with OSS software from Pronto Networks. And that's not all. For years, Sun has developed servers and storage for the challenging demands of telecommunication carriers. From its NEBS-compliant Netra server products and its highly-scalable UltraSPARC processor-based Sun Fire servers, to its economical, high-performance x86 architecture servers, Sun has a range of products to host operations support systems of all sizes. Sun believes in choice, and with Pronto Networks' software available to run on either UltraSPARC processor-based servers running the Solaris Operating System, or Sun's x86-architecture Linux servers, telecommunication carriers can choose the platform and operating system most appropriate for their environments. With OSS software from Pronto, and software, servers, storage, and services from Sun, those implementing public-access Wi-Fi networks have an easy choice of partners.

Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA **Phone** 1-650-960-1300 or 1-800-555-9SUN **Web** sun.com

The Network is the Computer™

Sun Worldwide Sales Offices: Argentina +5411-4317-5600, Australia +61-2-9844-5000, Austria +43-1-60563-0, Belgium +32-2-704-8000, Brazil +55-11-5187-2100, Canada +905-477-6745, Chile +56-2-3724500, Colombia +571-629-2323 Commonwealth of Independent States +7-502-935-8411, Czech Republic +420-2-3300-9311, Denmark +45 4556 5000, Egypt +202-570-9442, Estonia +372-6-308-900, Finland +358-9-525-561, France +33-134-03-00-00, Germany +49-89-46008-0 Greece +30-1-618-8111, Hungary +36-1-489-8900, Iceland +354-563-3010, India–Bangalore +91-80-2298989/2295454; New Delhi +91-11-6106000; Mumbai +91-22-697-8111, Ireland +353-1-8055-666, Israel +972-9-9710500 Italy +39-02-641511, Japan +81-3-5717-5000, Kazakhstan +7-3272-466774, Korea +822-2193-5114, Latvia +371-750-3700, Lithuania +370-729-8468, Luxembourg +352-49 11 33 1, Malaysia +603-21161888, Mexico +52-5-258-6100 The Netherlands +00-31-33-45-15-000, New Zealand–Auckland +64-9-976-6800; Wellington +64-4-462-0780, Norway +47 23 36 96 00, People's Republic of China–Beijing +86-10-6803-5588; Chengdu +86-28-619-9333 Guangzhou +86-20-8755-5900; Shanghai +86-21-6466-1228; Hong Kong +852-2202-6688, Poland +48-22-8747800, Portugal +351-21-4134000, Russia +7-502-935-8411, Saudi Arabia +9661 273 4567, Singapore +65-6438-1888 Slovak Republic +421-2-4342-94-85, South Africa +27 11 256-6300, Spain +34-91-596-9900, Sweden +46-8-631-10-00, Switzerland–German 41-1-908-90-00; French 41-22-999-0444, Taiwan +886-2-8732-9933, Thailand +662-344-6888 Turkey +90-212-335-22-00, United Arab Emirates +9714-3366333, United Kingdom +44-1-276-20444, United States +1-800-555-9SUN or +1-650-960-1300, Venezuela +58-2-905-3800, or online at sun.com/store

 Printed in USA 00/00 XX0000-0/#K