APPLICATION NOTE

The Alcatel-Lucent OmniAccess 8550 Web Services Gateway

AUTOMATED WORKFLOW FOR IMPROVED PATIENT CARE

Abstract

Healthcare institutions around the world want to provide high quality patient care while reducing medical errors and patient wait times. Many healthcare institutions are struggling under the weight of obsolete, manual business processes with little integrated IT system support. Studies show front-line healthcare providers spend only a third of their time with patients and the rest wrestling with inefficient processes. High quality patient care means deploying leading edge IT systems that automate healthcare provider workflow and streamline operations. Patient care provided at remote locations, such as clinics or private offices, can be significantly improved with online access to patient records.

Business process automation brings the increased burden of complying with information privacy regulations that have been put into place by many countries across the globe. The key issue is ensuring information privacy while also providing information that enables healthcare practitioners and support personnel to become more efficient - easy and secure access to patient records is essential.

The Alcatel-Lucent OmniAccess 8550 Web Services Gateway (WSG) is a network appliance that secures automated business processes to meet corporate governance obligations. It protects sensitive corporate data from misuse and ensures data is always available when and where it is needed. The OmniAccess 8550 WSG enables a network embedded SOA backbone that provides IT system interoperability for corporate wide security and regulatory compliance within healthcare institutions and enables the creation of an extended healthcare ecosystem that complies with strict governance requirements. Access to information is controlled through a corporate wide security infrastructure for Web service management that uses Alcatel-Lucent patent-pending message inspection technology.

Table of Contents

Introduction

The goals of healthcare institutions include providing leading edge patient services, improving operational efficiency and meeting new government information privacy regulations. In many hospitals across the globe, caregivers struggle with inefficient manual business processes and increased security requirements from information privacy legislation. Hospitals need to address the security requirement created by the need to automate caregiver workflow by enabling the flow of sensitive information between IT systems within their organization and with healthcare partners, such as insurance companies and contractors.

As a result, healthcare organizations are looking for ways to automate their business processes while respecting compliance requirements for information security. The ability to safely provide sensitive data when and where it is needed significantly increases the ability of highly skilled caregivers to spend time with patients, rather than wrestle with paper-based processes.

Standing in the way of these goals are the legacy information systems — clinical systems, human resources, enterprise resource management, finance — each of which maintains different security implementations. This situation impedes the flow of information required for effective business process automation. Automating business processes across dispersed locations or with healthcare partners presents additional secure information flow difficulties.

Web services have been promoted as a solution for organizations struggling to place existing business processes online and to automate business processes with partners. Unfortunately, the promise of Web services has been largely unfulfilled. While Web services do enable information flow, they also break down the security provided by each information system, and they do not provide a replacement mechanism for ensuring information security and compliance. As a result, many Web service implementation projects incur significant custom development and ongoing operational costs to maintain information security — and are not scalable.

The Solution: Deploying Web services using an SOA Backbone

A network-embedded, services-oriented architecture (SOA) backbone is a new approach that provides the corporate-wide compliance infrastructure required for scalable, business process automation. An SOA backbone is application-independent, enabling a consistent information access policy for all users. The SOA backbone also ensures that policy is enforced at run time across the organization as well as for business partners. This drives significant efficiencies in the definition and ongoing maintenance of information access control policy, reducing TCO.

The Key: The Alcatel-Lucent OmniAccess 8550 Web Services Gateway

The Alcatel-Lucent OmniAccess 8550 Web Services Gateway is a network appliance implementing an SOA backbone that provides IT system interoperability (Emergency, Radiology, Outpatient Clinic, HR, Finance) for corporate-wide security and compliance, enabling scalable, secure business process automation. Alcatel-Lucent's OmniAccess 8550 WSG ensures sensitive data is protected from misuse while allowing this data to be made available when and where it is needed, employing unique, session-based (multi-transaction) run-time policy enforcement and consolidated audit trails to guarantee compliance. Based on patent-pending Web services message inspection technology, the OmniAccess 8550 WSG is deployable both within a data center for internal information systems interoperability, and in a DMZ, extending interoperability to external networks such as laboratories, clinics and reimbursement partners.

Feature	Function	Benefits
Regulatory Compliance Demonstrate compliance and enforce conformance	• Provide consolidated audit trail to demonstrate complance • Provide run-time policy enforcement on end-user activity to provide application access control	• Offers unique, session-based (multi-transaction) policy enforcement technology to provide consolidated audit trails and run-time policy enforcement. • No manual, costly intervention to provide audit trail • Enables proper corporate governance
Secure Private Data Ensure information is not misused	• Provide information access and change control • Provide run-time data encryption to ensure corporate data is kept private	• Offers unique user aware and stateful session-based policy enforcement for information access control • Provides a single point for information access and encryption • Corporate-wide solution that reduces risk
Single Identity Single digital identity valid internally and with business partners	• Provide authentication with single sign-on internally • Provide authentications to trusted partners • Accept authentications from trusted partners	• Cost-effective identity interoperability via run-time translation rather than forcing a common identity management scheme • Allows independently set access policies • Maintains individual identity stores for each healthcare provider partner • Enables cross validation from one partner to another
Secured On-Line HealthCare ecosystem Provide automated partner ecosystem while ensuring the privacy of corporate data and identities without compromising traceability	• Safely exchange private information while maintaining traceability • Provide a single point for control and audit of all on-line partner activity • Provide seamless access to applications and information for authorized partner employees	• Enables highly-automated healthcare provider partner ecosystems with seamless service access • Ensures privacy of corporate data and identities, without compromising traceability • Offers unique identity interoperability technology that enables run-time user authentications among partners – end-to-end • Enhances productivity through seamless service access
Total Cost of Ownership	• Reduce the high cost of managing corporate-wide policy • Reduce the high cost of manual compliance audits	• Enables corporate-wide policies for the control and monitoring of information flow

Common Applications for the OmniAccess 8550 WSG in Healthcare

The OmniAccess 8550 WSG has many applications in healthcare including:

- Unified service access control
- Electronic reimbursement
- Contractor identity management
- Secured remote access to patient records
- Virtual electronic healthcare record creation

The following sections go into more detail on the important issues surrounding these applications and how the OmniAccess 8550 addresses them.

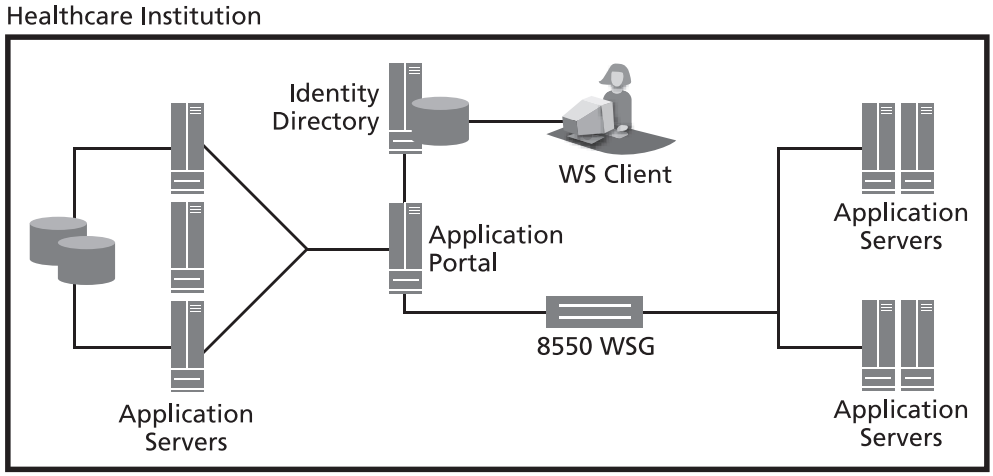
Unified Service Access Control

Healthcare institutions often use multiple information systems to support clinical, financial and other functions. These systems frequently maintain internal digital identities and user roles that do not map easily between systems. This leads to multiple logins for healthcare professionals to perform their work and it inhibits administrators from creating consistent and enforceable application access policies.

By exposing individual IT system functions using Web services technologies, healthcare institutions can create a service layer that allows creation of new and efficient workflows. The OmniAccess 8550 WSG installed in the data center provides a complete SOA backbone for Web services that enables interoperability between end systems with consistent access policies, enforced at run time, and consolidated audit trails of all activity. In this application, the OmniAccess 8550 WSG provides session-based policy enforcement, service mediation, and service monitoring and auditing for authorized service access.

Figure 1 shows the OmniAccess 8550 WSG deployed in the data center of a healthcare institution and enabling secure and manageable interoperability between information systems.

Figure 1: Unified Service Access Control for Hospitals



In this example, a healthcare professional at the healthcare institution accesses the local application portal to retrieve a patient's medical record and schedule a procedure for the patient. To provide this functionality, the portal connects through the OmniAccess 8550 WSG to Web services offered by two separate back-end applications. The OmniAccess 8550 WSG provides identity interoperability, authorizes service access via run-time policy enforcement, provides message transformation and creates a consolidated audit trail of all transactions. This reduces costs, provides traceability and allows the healthcare institution to enforce conformance to government regulations.

Electronic Reimbursement

Current insurance claim processing involves many different processes, including CD shipping. Electronic connections to insurance companies, if they exist, use old and expensive technologies, such as EDI, and require lots of manual effort. This is very costly and error prone. Adding new electronic connections requires custom development since EDI is a proprietary protocol not supported directly by information systems. Manual CD creation and shipping is not only pricey but it creates tremendous data privacy exposure due to the lack of control over the physical CDs containing patient information.

By installing the OmniAccess 8550 WSG in the DMZ, a healthcare institution can create a low-cost, secure electronic connection between its billing system and insurance providers. This connection uses Web services technologies with open standards that are supported directly by many information systems. In this application, the OmniAccess 8550 WSG acts as an application firewall allowing only valid Web service requests to enter the hospital's network. It also provides service virtualization, session-based policy enforcement, service mediation, and service monitoring and auditing for authorized service access.

Figure 2: Electronic Reimbursement for Hospitals

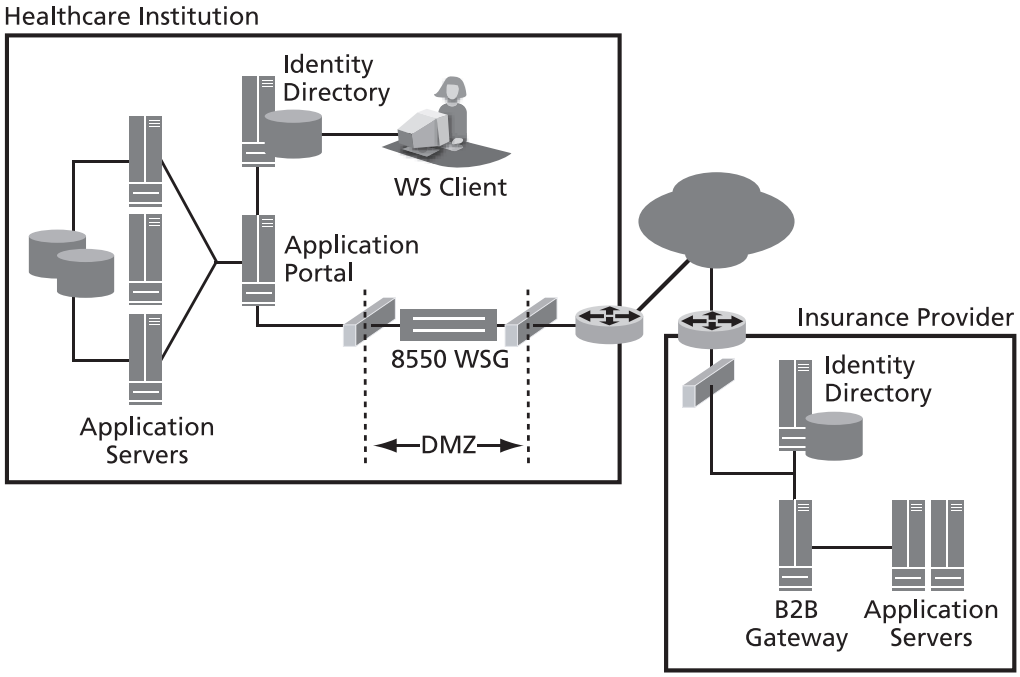


Figure 2 shows the OmniAccess 8550 WSG deployment in the DMZ of a healthcare institution enabling interoperability with an insurance provider.

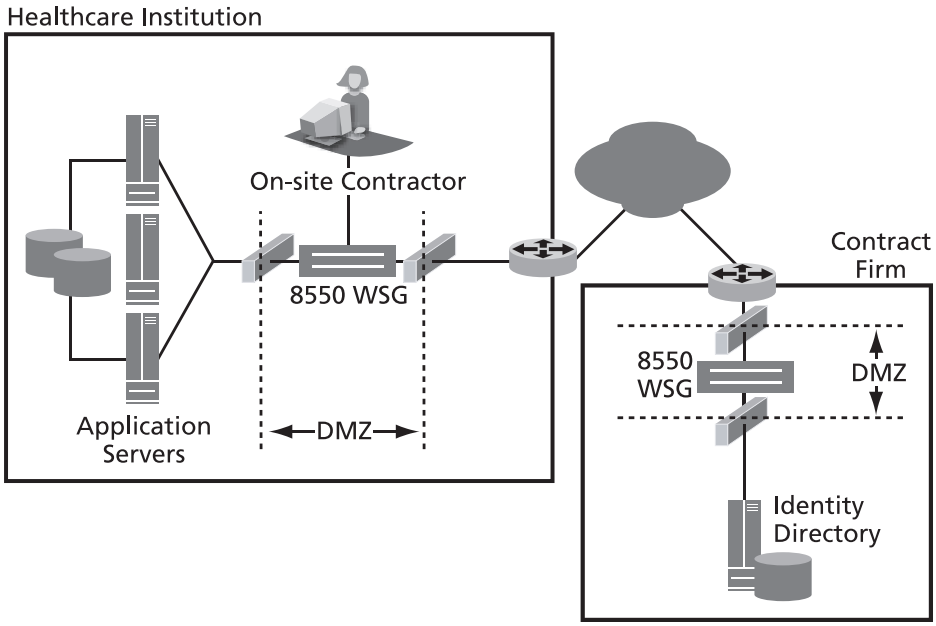
In this example, healthcare institution administrators access the local application portal and request current status reports for all reimbursement claims with the insurance provider. To provide requested reports, the application portal will connect to a claim processing Web service published by the insurance provider and proxied for use at the healthcare institution by the OmniAccess 8550 WSG. The OmniAccess 8550 WSG provides identity interoperability, authorizes service access via run-time policy enforcement, supplies message transformation and application data protection and creates a consolidated audit trail of all transactions. This application reduces costs, provides traceability and allows the healthcare institution to enforce conformance to government regulations.

Contractor Identity Management

Currently, hospitals maintain local identities for contract employees, such as medical transcribers, consultants, X-ray technicians and financial auditors. They often have no visibility into the actual employment status of these individuals. Yet legal liability rests with the hospital when contract firms do not update their employees' status. Furthermore, contractor activity often cannot be directly traced to the individual. This is a common problem reported by healthcare organizations and represents a very large corporate governance risk in complying with patient record privacy legislation.

The OmniAccess 8550 WSG installed in the DMZ of the healthcare institution and their partners as shown in Figure 3 enables a unique answer to this problem.

Figure 3: Managing Secure Access for On-site Partner Employees



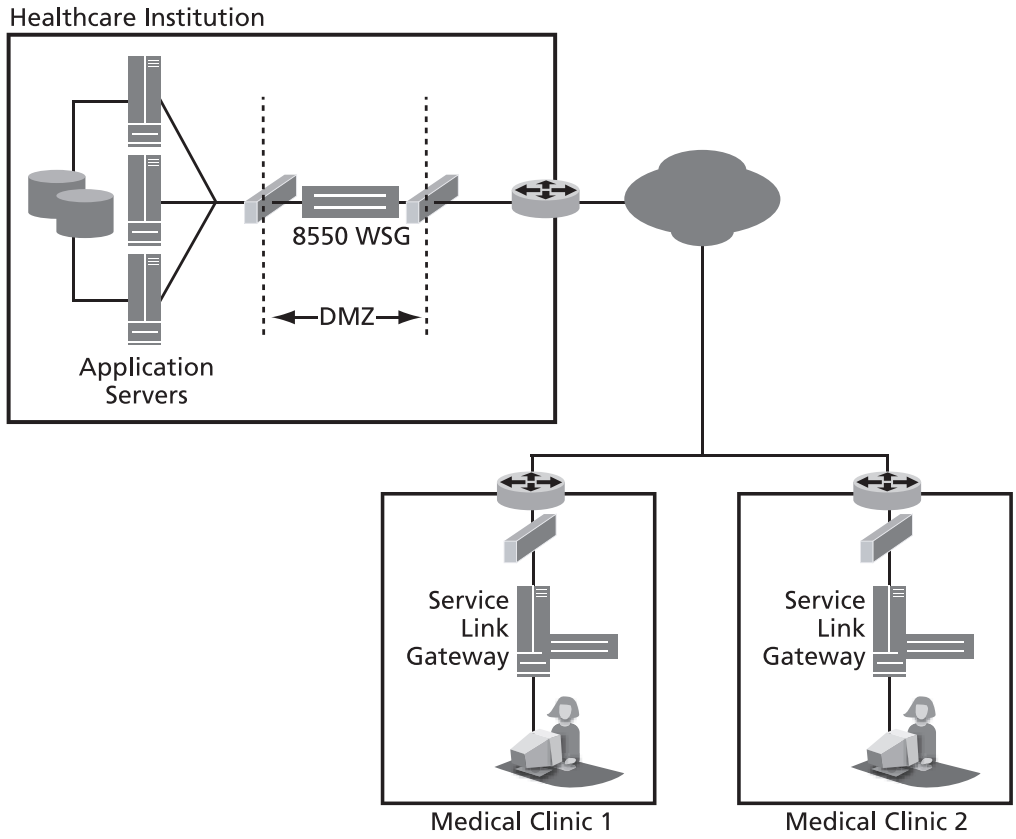
The OmniAccess 8550 WSG maintains secure connectivity with each partner and enforces policies indicating which Web services partner employees have access authorization. When a partner employee is on-site, the OmniAccess 8550 WSG at the healthcare institution relies on OmniAccess 8550 WSG at the partner site to provide remote user authentication. This allows the healthcare institution to provide secure access to partner employees when on-site, only when they are authenticated by their own employer. Legal liability for employee access remains with their employer, and provides completely traceable activities for those employees.

For example Mary, a partner employee, while onsite at the healthcare institution needs access to the same Web services she accesses at her own office. Upon connecting to the visitor LAN at the healthcare institution, Mary has all messages routed to the OmniAccess 8550 WSG in the DMZ of the healthcare institution. Mary identifies herself as a partner employee to the OmniAccess 8550 WSG and provides authentication credentials supplied by her own employer. The OmniAccess 8550 WSG at the healthcare institution forwards the authentication request to the OmniAccess 8550 WSG in the DMZ of the associated partner for validation. If the remote authentication request is successful, the OmniAccess 8550 WSG at the healthcare institution proxies access to all Web services for which Mary is authorized.

Secured Remote Access

Access to medical data from remote locations must be compliant with government information privacy regulations and access to records must be traceable via an audit trail to assess legal liability in the case of a "leak." Current methods of retrieving information via telephone or fax are slow and expensive. Simply tunneling physicians through the external firewall does not scale economically, nor ensure compliance to regulations, nor does it create a consolidated audit record.

Figure 4: Securing Remote Access to Web Services



With the OmniAccess 8550 WSG installed in the DMZ of a healthcare institution, as shown in Figure 4, the healthcare institution can provide access to their Web services at external medical clinics and doctors' offices to deliver patient records and other services. The healthcare professionals at these locations are known to the healthcare institution, but the clinics are not on the healthcare institution's corporate LAN. It is essential for healthcare institutions to secure access to these distributed locations without compromising network or application security and to ensure all service and data access remains compliant with government regulations.

In this example, a physician at medical clinic 1 can request a Web service that provides an individual patient's medical history. The physician then requests a service that summarizes all hospital-related activity by the physician in the previous month. These Web services are published by the healthcare institution to remote locations via the OmniAccess 8550 WSG. The OmniAccess 8550 WSG authenticates users, authorizes the service accesses, provides application data protection, monitors service performance and creates a consolidated audit trial.

Virtual Electronic Healthcare Record

The healthcare system currently has a fragmented patient healthcare record system. Each time a patient visits a healthcare facility treatment details are recorded and stored at the facility. As the patient visits different facilities, a new record is created at each location. Manual requests must be made from one facility to another to obtain complete patient information. It is also difficult to ascertain whether all facilities that provided care to the patient have been contacted, and submitted all data. Also, data can be lost due to the wide variety of formats.

The result is that healthcare professionals are unable to obtain all the information they need in a timely, cost-effective way and patient care suffers. For example, a patient's records may largely reside in their family doctor's database, which is inaccessible to hospital personnel. Or, any treatment obtained at the hospital may not be communicated back to the patient's family doctor automatically. The difficulty of sharing patient records is further compounded by strict privacy legislation. The healthcare facility that collects the data is responsible for protecting the data and ensuring only fully authorized people are able to access the data.

An Electronic Healthcare Record Solution (EHRS) with the vision of providing electronic access of all health records to healthcare providers while maintaining patient privacy is currently being implemented in North America and Europe. The goal is to improve patient care by allowing caregivers to have the complete health records of their patients. The interface to the EHRS is the Health Information Access Layer (HIAL).

The OmniAccess 8550 WSG can be included in EHRS at several locations in the architecture:

- Within the HIAL to provide interoperability between information services
- Provide interoperability between independent EHRS
- Secure remote access to the EHR from point-of-presence applications

The OmniAccess 8550 WSG meets EHRS blueprint requirements including identity management, inter - agency interoperability requirements, conformance to regulatory requirements (data privacy), automatic transformation between storage record format, and security requirements.

Advocate Health Care

Founded in 1980, Advocate Medical Group is one of Chicago's leading physician group practices, with more than 190 physicians providing a wide range of medical and surgical care. Advocate Medical Group physicians are on staff at Advocate Lutheran General Hospital, and some are on staff at Advocate Good Shepherd Hospital in Barrington. Advocate Medical Group physicians provide outpatient care and diagnostic services at 18 locations throughout the north and northwest Chicago area. Advocate Health Care supports a network of approximately 26,000 users of which 4,000 to 5,000 are expected to be active at any time.

Due to a lack of interoperability between various applications, many of Advocate's internal processes require extensive manual effort. Typically creating or updating a user identity for an information system involves downloading, filling out and printing a form, obtaining necessary signatures and mailing or faxing the form to an administrator who will enter the required data into the system. This type of process leads to long delays in fulfillment and is difficult to audit. By transitioning to a service-oriented architecture, Advocate can create new automated processes that create efficiencies in their operations. However, to realize the benefits of a SOA, Advocate needs the ability to scale service deployment with consistent policy enforcement and audit capabilities.

Advocate has electronic connections with numerous insurance providers and other agencies for reimbursement of patient care. Integrating with the diverse set of applications and custom data formats used by various insurance providers is difficult and costly. Maintaining private network connections and custom integration software with each insurer, and providing manual data consolidation are very expensive operations and yet are not sufficient to ensure compliance with government regulations. Transitioning to a Web services-based automated workflow

helps reduce the operational costs of claims processing. To benefit from this approach, however, Advocate needs a scalable and flexible interoperability of external services while maintaining application security and enforcing compliance with government regulations for all service and data access.

Also, Advocate must provide access to their network and information systems to employees of various external companies regularly. In particular, Advocate contracts medical transcription services from multiple small companies and allows employees of these firms access to patients' medical records while they are on-site at Advocate. To provide this access Advocate must maintain digital identities for these contractors in their identity management system, which does not always get timely updates on their employment status from the medical transcription firms. This represents a security and governance problem for Advocate, but there is currently no capability for the medical transcription firms to authenticate their own employees directly while they are on-site at Advocate. Allowing portability of digital identities between corporations is difficult, but necessary to provide proper governance at Advocate.

Advocate is looking to serve IT services to remote locations such as affiliated doctor's offices and local clinics — and to create a health - care ecosystem that serves patients at many points of presence to help integrate Advocates services firmly within the community.

With these challenges in mind, Advocate is currently evaluating the Alcatel-Lucent OmniAccess 8550 Web Services Gateway and intends to deploy when a production-ready version is available later this year.

Alcatel-Lucent Delivers Value to Healthcare Providers

For healthcare organizations striving to secure online business processes and automate business processes with partners, the Alcatel-Lucent OmniAccess 8550 WSG is a unique, scalable, low-cost solution to enable IT system interoperability with corporate wide security and regulatory compliance for effective and secure automation. Capitalizing on unique, patent-pending Web service message inspection technology, the Alcatel-Lucent OmniAccess 8550 WSG offers many features currently unavailable in the market. The OmniAccess 8550 WSG significantly reduces the total cost of ownership (TCO) for information systems.

The Alcatel-Lucent OmniAccess 8550 WSG is unique in its ability to install a single institution-wide, network-embedded SOA backbone that provides an institution-wide compliance infrastructure required for effective business automation.

www.alcatel-lucent.com

Alcatel·Lucent