



Aztec Security Services

Creating More Business for You

Overview

The world is reeling under a recession and vendors of software applications are struggling to be in business. Business opportunities are rare and difficult to realize. Sales cycles are prolonged as customer decision-making process is now protracted.

Recession

November 30, 2001 <http://europe.cnn.com>

The U.S. economy shrank at a faster pace in the third quarter than initially thought, the government said Friday, as the world's largest economy put in its worst performance since the last recession more than a decade ago.

November 20, 2001 <http://europe.cnn.com>

LONDON (CNN) -- The global economy appears to have slipped into a recession for the first time in 20 years, the OECD said on Tuesday.

November 19, 2001 <http://www.cnn.com>

KUALA LUMPUR, Malaysia -- Malaysia is already in recession and the economic slump could get worse in the next six months as consumption slows, according to investment bank Goldman Sachs.

Given all these uncertainties, there still remains a gold mine of opportunities for vendors who are receptive to the market's current needs. Application and Data Security, for instance, has become the focus and a lot of investment is anticipated in this area.

Heightened Concern about Security

October 24, 2001 – <http://www.cnn.com>

ORLANDO, Florida (IDG) – “In the wake of last month's terrorist attacks, IT managers and industry experts at the Storage Networking World conference here say.....

Companies are in danger of being sued if a customer's data is stolen or "hijacked" and damages result from the release of information

We at Aztec have proven expertise in application security. We can help you enhance the security of your applications adding one more value proposition for your customers to sign up with you.

About Aztec

Aztec (www.aztecsoft.com) is into providing **customized software engineering solutions, maintenance support and total testing solutions** to enterprises and new economy players like B2B marketplaces, B2B service providers, and Internet product/infrastructure services companies. Our development base is in Bangalore and we have marketing offices all over the world. We are listed in BSE, India.

We have developed this expertise while working as partners for companies like Asera, Jamcracker, **Microsoft**, **IBM**, Embarcadero Technologies, **Novell**, and Viador.

Our application security experts work in these areas:

- Authentication
- Authorization
- SSO
- Developing PKI based applications
- PKI enabling of applications
- Directory services based security
- User management solutions
- Wireless security.

Our Service Offerings

Following is the list of things that we can do to enhance the security of your application:

- PKI enabling of applications
- Single Sign On enabling of applications
- LDAP enabling of applications
- Authentication services solutions
- Authorization services solutions
- Standardizing the security mechanism in an application for higher interoperability and compatibility
- Audit and logging
- Consultancy on improving the overall security of an application from design to code

Elaborate Infrastructure

We have a state-of-the-art communication infrastructure comprising:

- A dedicated point-to-point link connecting the Bangalore, India, facility to a data center at Santa Clara.
- A T1 line that connects the US and India offices to this dedicated line.
- T1 lines that connect our clients (if required) to this dedicated line.
- A reliable, high-speed link from our office to client locations set up to improve productivity.
- A 512K BPS leased line from the Bangalore facility for general-purpose Internet use.
- Internal LAN with NT, Solaris and Linux nodes.
- Windows and Solaris development tools and most of the popular commercial RDBMSs.

PKI Enabling Of Applications

The following components of an existing application can be integrated with PKI. However a given application may not have all of the following components.

- **Browser Front End**
 - Integrate support for existing PKI into browser for import/export of keys/certificates, digital signing and strong authentication
 - Key generation - Integrate support for various storage media such as smart cards, tokens etc
- **Authentication and Access Control**
 - Provide strong authentication to the application by using public key cryptography available through PKI. In this scenario, the client can carry credentials on hardware tokens and devices (further protected by biometric) thereby making the authentication very secure.
 - Since PKIs are usually well integrated with an LDAP based directory service, we will leverage the directory to store authentication information in a logical fit for you. It provides a well-integrated authentication and authorization component.
- **Web Servers:** Integrate server side PKI functionality into web servers such as:
 - Signature verification
 - Checking for revoked certificates
 - Mapping authenticated identities to certificates
 - Managing secure sessions

- **Single Sign-On (SSO):** PKI also offers the solution in the areas of Single sign on for its user. Normally by installing and configuring PKI server, you do not get SSO functionality. The application has to be PKI SSO aware. We will enable your application to be PKI SSO aware.
- **Document Signing:** Document signing is an essential part of e-commerce and needs to be implemented at most of the stages. We will enable security and non-repudiation solution for your application using PKI.
- **Secure Communication and Messaging:** Secure communication between applications and with user will be achieved using PKI authentication and secure communication.
 - SSL can negotiate encryption keys and authenticate the server before data is exchanged by the higher-level application.
 - The SSL protocol maintains the security and integrity of the transmission channel by using encryption, authentication and message authentication codes.
 - SSL can be also used to provide client authentication.
 - SSL enabled applications can communicate with users or other applications by using their own certificates and ask for other party certificates.
 - Secure e-mail, messaging and groupware applications may encrypt messages and files and use digital signatures, to ensure authentication, privacy, and data integrity.
 - EDI systems can use PKI for financial transactions.
 - The IETF standard secure e-mail/messaging protocol is Secure Multipurpose Internet Mail Extensions (S/MIME), which extends the Multipurpose Internet Mail Extensions (MIME) standard. S/MIME can use PKI to digitally sign messages and to encrypt messages and attachments.

Service Benefits

Benefits of getting your application PKI enabled from Aztec are as follows:

- Your PKI enabled application will meet your current and future security needs
- You will get access to a well integrated infrastructure
- Your application's security will achieve interoperability with the security of PKI enabled applications from other vendors.

Single Sign On Enabling of Applications

The Single Sign On (SSO) service offers to enable the suite of applications for a one-time login by the end-user. Though SSO has been around for a while, there are many different ways of achieving SSO, and not all of them are secure and without problems. Every solution has its advantages and disadvantages. Depending on various factors listed below, some of the solutions fit the bill better than others:

- Nature of the applications
- Their deployment environment
- End-user usage considerations
- Budget constraints

Aztec has immense experience in almost all of the known/available SSO technologies and tools. This puts us into an ideal position to understand the application(s) to be SSO enabled, and suitably adopt the best approach both from technical and business perspectives.

As a part of the overall offering, we provide the following services to the customer:

- Provide product requirement recommendations after a careful analysis of the application architecture & design, and the technology & business requirements
- Architect and Design the SSO solution for the application(s)
- Implement the design by way of developing the SSO modules and integrating them with the mainstream application(s)
- Test the solution for functionality, security, scalability and performance.

Methodology

The methodology of Single Sign On is multi-pronged and is narrowed down to a set of technologies/tools that best suit the given conditions, as explained above.

At a very broad level of classification, we classify SSO into two categories, namely, Web-based SSO and Enterprise SSO. Web-based SSO deals with technologies and products that provide Single Sign On to Web-based (browser based) applications. On the other hand, Enterprise SSO technologies and products tie all network, client-server, and intranet applications into one single authentication thread, thereby providing Single Sign On. In each of the categories we further break down the problem into various scenarios.

Web Based SSO Scenarios

- A product suite consists of many web-applications, each of which requires SSO authentication. Also, all the applications and the SSO system must be deployed within the same firewall.
- A product suite consists of a few web-applications, and SSO is required across them, as in the above case. Additionally, a capability for other external web-based applications needs to exist such that they can sign into the SSO system of the original application suite.
- SSO across two or more web-applications that can communicate only over the internet, but the SSO system needs to reside at a totally separate location, accessible only over the internet.

Enterprise SSO Scenarios

- There are many Unix based client-server applications that need to be SSO enabled. Also the clients of these applications are not modifiable, whereas one has the flexibility to work only on the server side.
- There are a host of applications (both client-server based, and stand-alone) and one does not have the flexibility to modify them at all. However SSO is required across these applications.
- A product, when deployed in a Win 2000 environment, should delegate its authentication to the NOS, i.e. Win 2000, by leveraging the Kerberos technology available in Win 2000.
- A product needs to SSO enabled in conjunction with a given directory service sign-on, such as iPlanet Directory, Novell eDirectory or Microsoft Active Directory.

There could be more such scenarios.

We gather a thorough understanding of the technical and business requirements of the customer, and design the solution that is most appropriate. The solution may also leverage functionality and features provided by a wide variety of tools available from popular commercial vendors such as Netegrity, Entrust, Novell, and Microsoft.

Unique Technology Propositions

The SSO Service adds to the user convenience, but it also raises new security concerns. Some of the SSO approaches mentioned below raise very serious concerns about the security of the system. Password Synchronization solutions are vulnerable to the weakest-link-security problem, where the confidentiality of the entire range of applications depends on the system with weakest security. Moreover, such solutions are very complex in design and difficult to implement and manage, and have a low response time.

Some solutions attempt to store passwords on client workstations, in a poorly encrypted manner, such that the user secrets can be quickly recovered by using hacking tools widely available on the Internet. One such example is the Windows "Remember the password" technique.

We are very wary of such scenarios, and our solution design solves problems, more than it creates.

We are not the run-of-the-mill operators who use the same technology and solution for all requirements. Neither do we solely rely on SSO products to achieve the solution. We use the products only when they pass the technical, business and budget analyses. We have the capability to build SSO solutions entirely on our own to limit costs without sacrificing quality and features.

To sum up, *"we do not sell a solution, we engineer it."*

SSO Tools and Technologies

We have expertise in these tools and technologies:

- Netegrity SiteMinder
- Entrust getAccess
- Kerberos based SSO (both the Windows 2000 and regular Unix implementations)
- Novell SSO
- MS Passport
- Tivoli Global Sign On
- PKI/Smart Card based SSO
- Oblix SSO solution

SSO Service Benefits

Some benefits of providing SSO are as follows:

- Significant reduction in password-related support costs for your customer
- Better and simple end user experience. The end user need not log in twice to access two different applications bought from you.
- Better network security
- Faster user access to data and applications

LDAP Enabling of Applications

Your application will be LDAP-enabled by integrating it with an LDAP directory. Your application will get to leverage the various benefits of an LDAP Directory Service.

Some of the benefits of LDAP Directory Service are highlighted below.

- Secure User and Profile Management
- Strong Multi Factor Authentication
- High Availability of data
- Distributed information management

LDAP Services

- Certificate Services
- A highly fine-grained Authorization System for maximum security
- Policy based Application Auditing
- Application personalization for a user by managing a master index of user profile

LDAP Tools and Technologies

- iPlanet/Netscape Directory Service
- Novell eDirectory
- Microsoft Directory Service
- OpenLDAP Directory Service

LDAP Benefits

- Lets you focus on your core business logic rather than diverting your focus to existing technologies (such as User Management, Security)
- You do not have to reinvent the wheel
- Based on Internet standards (LDAP, X.500)
 - So interoperability and global acceptance is guaranteed
 - Frees you with the burden to keep in sync with latest advancements in Security and User Management technologies
- Let the Directory Service do it for you, so that you always have the latest technology.

Authentication Services Solutions

Authentication is a process by which a system recognizes a requester's identity and decides user access to system's resources using some predefined rule.

Aztec software has done extensive work to enable state of art Authentication system. Aztec has also developed a huge library of components and products in this line, which are currently being used by many customers. Hence you get a solution that has been tried and tested and one that reduces the development time.

Following are the functionalities of authentication systems technology in which Aztec excels:

- Implementation of multiple authentication schemes. Like,
 - User ID
 - Hardware token such as RSA ID (Two factor authentication)
 - Smart Card
 - X.509 certificate authentication
 - Biometrics solution integration
- Single Sign on to Web Application and multiple applications across domains.
- Directory enabled and RDBMS supported.
- Real-time session management.
- Mobile authentication for different mobile device.
- Auditing and logging all events.

Service Benefits

- Robust security for your applications as we use the latest technology advancements in biometric authentication, proximity recognition, password management and public key infrastructure (PKI).
- Your application can provide universal user access from virtually anywhere to all authorized systems and databases
- Flexible and scalable deployment
- Rapid implementation that leverages the existing IT infrastructure
- Low cost of ownership
- Extensible authentication framework to which any kind of new authentication technology such as SmartCards and Biometric solutions can be fit in.

Authorization Services Solutions

Authorization, an essential part of any system, controls user access to system resources on privilege basis. Aztec has vast knowledge in this area and has implemented solutions for numerous customers. In the process, we have developed components and frameworks that can be easily adapted in future assignments.

Key features of our authorization services are as follows:

- Controls access at a fine grained level
- Provides role based access control to different operations on different Business Objects.
- Is independent of any platform and backend technology
- Provides distributed authorization information management
- Accommodates any new organizational structure such as groups, department or hybrids. The framework is highly scalable.
- Works with LDAP and RDBMS

Unique Technology Proposition - Aztec solution of Authorization using LDAP

Aztec Access Control List System (AzACLSys), an authorization system, implements the "Access Control Model for LDAPv3" RFC. This access control system evaluates requests for access to protected resources and makes decisions about whether those requests should be granted or denied. In order to make a grant/deny decision about a request for access to a protected resource, an access control mechanism needs to evaluate policy data. This policy data describes security-relevant characteristics of the requesting subject and the rules, which govern the use of the target object.

AzACLSys system has a few special characteristics:

- It follows the directory hierarchy structure in deciding user privilege to a target object.
- AzACLSys follows object inheritance of directory tree, which adds a great potential to an Authorization system. It means that object inherits its parent's attributes and characteristics. Additionally, a child object can override inherited characteristics and define their own effective prominent ones. AzACLSys system makes decision by considering ACLs (Access Control List) precedence, location and type into account.

Implementing Standards-Compliant Security

Aztec offers services to standardize the security mechanisms existing within applications for better interoperability and compatibility. Some examples are:

- Integrating SSL for secure communication
- Integrating S/MIME for secure messaging
- Integrating PKCS based PKI
- Integrating GSS support for authentication and communication security
- Integrating LDAP based authentication and authorization

Audit and Logging

Aztec offers services to build auditing and logging functions into your existing applications. Most applications do not have much functionality built into them thereby leaving a big area of security unaddressed. Aztec can study the design of the application and design and develop secure auditing / logging / reporting component for the application.

Aztec also offers ready 'Auditing framework' that integrates with most enterprise and web based applications written in C/ C++ or Java programming languages. The applications being enabled need to expose an API / SDK for our framework to plug in. If this is not feasible, it is still possible to leverage the 'Auditing framework' however with some development overheads over and above the base framework.

Methodology

- Requirements gathering
- Study of application to be enabled
- Design and development of Auditing & Logging component
- Integration of Auditing & Logging component with the application
- Acceptance testing and delivery
- Support

Service Benefits

- Secure Audit trails for all events within your application
- Secure storage of these audit trails
- Prevents even system administrators from tampering these trails
- Enables complex queries and searches on the audit trail
- Auditing based on detailed policy setups to govern what to audit and under what circumstances.
- Integration with popular reporting mechanisms

Note: A lighter version of this auditing framework is also available.

Consultancy to Improve the Overall Security of an Application

Aztec can provide consultancy in developing a secure application from design process till the product deployment. A few typical areas in which Aztec can provide consultancy services are listed here:

- Design the application from scratch

While designing your application, we will carefully consider the environment in which your application will run, the input and output behavior, files used, arguments recognized, signals caught, and other aspects of behavior.

- Review your program code for security purpose and suggest improvements. Some of the things that we will look for are as follows:
 - Make the critical portion of your program as small and as simple as possible.
 - Check configuration dependencies
 - Check deadlock conditions
 - Check sequence conditions
- Study your application to identify the security loopholes and suggest solutions. Some of the aspects that we will look for are as follows:
 - Check all input and output parameters to system

Security-related bugs arise when an attacker sends an unexpected value or an unanticipated format to a program or a function within a program. To avoid these issues, you must ensure that all the arguments input to your programs are verified. Argument checking will not noticeably slow your application, but it will make the application less susceptible to hostile users. You must ensure that these checks are performed by your application:

- Check arguments, which are passed to operating system functions. Even though your program is calling the system function, you must check the arguments to be sure that they are what you expect them to be.
- Check all return codes from system calls.
- Develop internal consistency-checking code.
- Check serious security glitches by:
 - Creating program dump core except during your testing.
 - Creating files in world-writable directories.
 - Placing undue reliance on the source IP address in the packets of received connections
- Put reasonable time-outs on the real time application and user sessions.
- Put reasonable limits on the CPU time used by your CGI script while it is running.
- Include some form of load shedding or load limiting in your server to handle cases of excessive load.

Our Commitment to Quality

We at Aztec believe that the only way for us to grow is to grow with our customer. The commendation mails from our customers are such a frequent occurrence that they do not raise eyebrows any more!

Octago (www.octago.com)

"...This is a major milestone achieved, and we at Octago are delighted and extremely excited. It is like seeing a child being born... you continue to prove that if anyone can do it - you can.... You continue to impress us with your professionalism, enthusiasm and commitment. I am proud to work with you all "

iMediation (www.imediation.com)

"...iMediation is very satisfied of the work performed by Aztec on this work package. The engineers that you have sent here have showed that they were fast to understand our product and have later, with their colleagues, proposed valuable enhancements to the test plans..."

Microsoft (www.microsoft.com)

"...Our initial project with them was for 2 years... This speaks very highly of their understanding of database technologies in general, and SQL Server technologies in particular. We are very happy with their work and continue to work with them on a long term basis..."

Features of our Service

- We have a huge library of ready-to-use components, which cuts down on development time.
- We have built our security expertise on top of deep expertise in Data Management, Integration and Internet Middleware. Hence you get access to specialists in security who can also see the holistic picture.
- Proven project management process
- Defined, iterative software development methodology.
- Immediate, 24/7, access to Security experts
- Assigned team with deep technical expertise and flexible working style.
- Excellent documentation
- Excellent support
- Reliable backup and recovery

Benefits of Working With Aztec

- High-quality solution ensured by deep technical expertise, proven processes and stringent testing.
- Ease of execution with tested global delivery model.
- Rapid delivery and hence providing you the Early-mover's advantage.
- You get additional business by highlighting the security aspect of your products
- Cost-effective solution

Customer Case Studies

Asera Inc.

Based in Belmont, Calif. Asera (www.asera.com) offers an e-Business Operating System. It comprises two essential technologies:

- A platform of software services to deploy and run the solution,
- A development workbench to build and manage it.

The Asera Platform, coupled with best-of-breed foundation technologies, provides an architecturally robust and rich set of services that enables an organization to design and automate business processes independently from any particular set of applications. The various applications couple to the Asera platform and the users has to access the various applications through the Asera platform. Hence the organization achieves application independence and the user is provided with a seamless experience. The organization gets to leverage the data and logic of multiple, disparate applications.

The partners of the organization are the various business partners - supplier, resellers etc. The users are the employees of the organization or it's partners.

Aztec's Asera Assignment

The Asera platform offers the ability to construct composite applications using workflow, presentation and business objects. As part of this workflow, the platform had to offer an Access management layer that provides:

- A framework to manage users and user's access to resources and data at coarse and fine levels.
- A framework that is easily configurable and customizable to tailor to specific deployment needs.
- A complete set of runtime web-based administrative tools that lower maintenance costs.
- An extensive and rich library of APIs for authentication, authorization and entitlement.
- Support for a complex B2B environment with relationships between trading partners.

Aztec's Solution

We categorized the solution into Single Sign on, Authentication, Authorization, User management, and Encryption and Data store independence.

Single Sign On

Single Sign On requires that a user is able to sign on once to the Asera system. Based on their authorization, the user is able to see links to applications outside of Asera. The user can choose any of these links and go to each of these external applications seamlessly without having to login once more into that external application. Key features of the SSO Solution are as follows:

- Supports transparent logins to provide seamless navigation across composite applications.
- Provides an administration application to add new applications that are SSO enabled and create resources for these new applications. The administration application also captures authentication, authorization and encryption information for the new application.
- Tracks SSO applications that a user has accessed in a session. It handles idle and session timeouts.
- Manages user accounts and passwords.

Authentication

This is the process of establishing a user or partner's identity before determining what they can do in the system.

- The solution leverages the Asera Adapter/Connector architecture to provide authentication using an external authentication product that can be either Netegrity SiteMinder or Entrust getAccess depending on the requirement of Asera's customer.

- The solution supports authentication by Digital certificate besides userid/password.
- The solution defines and implements APIs to support external authentication products
- The solution supports system/application access

Authorization

Authorization is the process of determining what an authenticated user or partner is allowed to do in the system. The solution

- Provides ability to define user and partner profiles to use in rule based entitlement
- Supports authorization to workflow steps and to static URLs.
- Leverages external authentication products for supporting authorization to static URLs.

User Management

User Management requires the ability to manage users, their preferences, groups and the user's authorizations.

- Designed and implemented a set of workflow based applications to manage users, groups, user preferences and settings and user's authorizations.
- Provided the ability to change localization settings and preferences.
- An organization is allowed to create groups that mirror partners, delegate authorization to child groups, limit scope of users in child groups to authorizations granted to that group only.

Data Store Independence

The solution supports persistence of user and user profile in either an Oracle Database or a LDAP Directory Server.

Standards

- Evaluated standards - SAML and JAAS to design the APIs for the framework.
- In the B2B environment, provided support for secure communication (HTTPS) between trading partners using the JSSE framework (supports different authentication mechanisms like username/password and digital certificates).

XML Global Technologies

XML Global Technologies, Inc. (www.xmlglobal.com) is a software developer and vendor of XML solutions. As an active member of XML standards initiatives such as OASIS, ebXML, W3C, and UDDI, XML Global fully supports the efforts of OASIS and the United Nations in producing the ebXML specification for the globalization of e-Business.

The Challenge

XML Global wished to build a web-based application, called Ceremony, which would provide services to store and verify electronic signatures on documents. The electronic signature mechanism itself was to be extensible, with an initial password-based implementation that would later be extended to cover other electronic signature mechanisms, such as scanned signatures and biometric signatures (for example, fingerprints and retinal scans).

The Aztec Solution

The Aztec team created a solution that met all of the Ceremony requirements, providing extensible mechanisms for securely capturing electronic signatures, verifying the same, and storing records of signatures performed in the Ceremony database. In addition, the Aztec team created a proof-of-concept for the Ceremony application, demonstrating how it could easily be plugged in to any existing application. The proof-of-concept was demonstrated by XML Global at a tradeshow and was very well received.