7M Aspire

Technology Overview

Technology Overview

Executive Summary

A key challenge for most enterprises today is to get real business advantage from their IT investments, such as opening new revenue areas, improving time to market or reducing operational costs.

Normally, the enterprise must deal with a variety of applications from different eras, ranging from mainframe and UNIX to Windows and new, Web enabled applications and information portals. Users are often geographically distributed in multiple business units, and they want secure access to their applications and resources independently of location and device.

Server centric computing has therefore had a renaissance. This model enables the organization to reclaim central control over mission critical and costly IT resources. Server centric products are maturing, but are mostly ignoring the scale of management problems involved in a continually changing organization. Organizations change through mergers and acquisitions, business units are continually calibrated against dynamic requirements, and individual users change roles, positions and projects. A key challenge is to manage this complex and constantly changing matrix of distributed applications and users in real time.

7M enables organizations to harvest business advantage by managing this complexity effectively, allowing rapid reaction to the business needs of the user. This is achieved through:

- A single web client integrated with the portal, providing single sign-on to any application backend from any location
- Central management of resources and application access
- License usage management and reporting
- Centralized or delegated administration of user profiles
- A turnkey solution that can be rapidly implemented

7M Aspire makes it simple to manage the access of many users in many locations to many different applications on different platforms. The robust infrastructure scales from individual business units to the entire enterprise, or even to external hosting services. This scalability has been tested independently at IBM laboratories.

For the end user, simplicity comes in the form of a web client that gives instant and secure access to all applications needed for your work. An individual application profile is available regardless of location, and a single log on gives access to many different systems.

Application management is divided into different layers. Whereas application access and license control is highly centralized to manage critical resources, user and profile management can be safely delegated to local administrators who can react rapidly to individual user needs. This is done without compromising the overall security and integrity of the IT infrastructure and with minimum training needs.

7M Aspire also enables organizations to implement the service provider model internally with minimum overhead. This can be combined with internal billing based on metered application usage.

Application Management

To make the Internet an important enabling technology for e-business, organizations are now building architectures to support scalable and reliable e-business applications. The creation of these architectures involves bringing together disparate platforms, operating systems, and applications into a coherent Internet presence. The new computing platform becomes the primary vehicle for delivering services to the entire enterprise value chain, comprising employees, business partners and customers.

Three important technology platforms have emerged to provide a coherent e-business platform:

- *Remote access software* that web enables existing Windows desktop applications running on central servers;
- *Application server middleware*, exemplified by products such as BEA WebLogic and IBM Websphere; and
- *Enterprise portals* as the fut ure web based desktop for employees, trading partners and customers providing a unified access point to all relevant information sources.

Figure 1. 7M Aspire application deployment portal

Enterprise Portals

Portals are often custom made solutions, although several *Information Portal* vendors have emerged in the market. These portals emphasize the organization of and access to information based on both structured and unstructured data. Some products also offer collaboration and information sharing capabilities. A new breed of desktops is also emerging, called *Enterprise Application Portals (EAP)*. These are process centric and seek to provide seamless access to, and integration of, new or existing applications.

Application portals are currently in their infancy. The market is strongly related to *Enterprise Application Integration (EAI)* tools and frameworks. Together, these hold the potential promise of unifying existing (legacy) and new applications by exposing business processes and integrating/extending these business processes using workflows.

However, current solutions are lacking in several respects:

- Providing an integrated approach to application management and delivery that takes into account the complexity of existing legacy systems
- Effectively managing a large number of distributed organizations and users by intelligently delegating appropriate administrative functions where appropriate
- Secure access and license control for all types of applications that are delivered inside the enterprise or to external customers and partners, including reporting and billing capabilities
- A single Internet application desktop that can either integrate with an existing information portal or be embedded inside such portals.
- Integration with emulation technologies for instantly delivering existing applications to web clients from mainframe, UNIX, and Windows backends
- An open and standards based framework for delivering small, web based components that access back end systems such as ERP, document management, collaboration and CRM systems

We call the solution that provides all these elements an *Application Deployment Portal*, the one stop solution for managing and deploying applications to a large user community inside the organization or across the Internet.

Functional Overview: End Users

End users log on to 7M Aspire through a web client to get a simple and browser integrated desktop that gives access to all applications from a single point. The application profile depends on the individual user's preferences, organizational roles and responsibilities, and the device from which the user is connecting.

From this web client, the user can access legacy applications from a variety of application servers, ranging from mainframes to Windows and Web. Emulation software enables the immediate delivery of such applications across the Internet, without any modifications necessary.

The applications can also be configured with single sign-on (SSO) to remove the support problems stemming from users having multiple login names and passwords to different applications. 7M Aspire includes a secure framework for managing the different accounts associated with a given user and thereby eliminating the need for

multiple logons.

Since users are accessing all applications through one secure channel, 7M Aspire is also capable of metering the individual usage of applications. All usage data are stored in a central repository. From here, these data can be used for generating reports on the application usage per users, departments or business units. Usage data can be used either for tuning vendor license agreements or for inter- or intra-company usage billing.

7M Aspire is designed according to open industry standards in order to integrate into existing infrastructures. The requirements and complexities of different organizations mandate such an approach. For example, users may already be accessing an existing information portal, e.g. through an organizational intranet. 7M Aspire can then be seamlessly integrated into this portal as a mechanism for managing and delivering mission critical applications to end users over the web.

Administrative Advantages

One of the main differentiating factors of 7M Aspire lies in the comprehensive administrative backend of the system. The goal has been to provide a single point of management for users and all their applications and information resources. Management should be simple, yet flexible enough to accommodate the different needs of organizations without extensive customization and tailoring. Moreover, administrative functions should be clearly separated according to roles to allow decentralized and delegated management without sacrificing overall security and control.

In 7M Aspire, administration and management is divided into two main tiers. On the back tier are the applications that must be provisioned to enable the centralized control and distribution across the Internet. From a single console, administrators can configure applications and control their appearance, security requirements and distribution mechanisms. This is typically done once per application. In addition, the administrator can define license usage rules associated with each application. These license rules typically define global access criteria. For example, an application can be configured to be available to all business units with a maximum of 5,000 concurrent users at any time. 7M Aspire provides great flexibility in defining new license rules from a business perspective.

The front management tier is concerned with the users and their access to applications. Given a specific number of application licenses, these can be allocated to users according to departments, roles and responsibilities, or dynamic groups such as project teams. The administrator can easily define new groups or roles, assign applications to these, and then allocate individual users to the groups. Users will then receive an updated application profile based on their membership in various groups and roles. If necessary, applications can also be allocated to individual users.

User administrators may also have the capability of creating new users or disabling existing ones. Each delegated administrator has management privileges in a defined administrative domain. In this way, organizations can define exactly the administrative granularity that is appropriate for them and assign local administrators to manage the day-to-day aspects of application access.

This decentralized model of user administration is essential to a real world system to prevent it from becoming an administrative bottleneck. Application access should be managed as close to the user as possible to improve the overall responsiveness of the system to the individual requirements of users and business units. At the same

time, the two-tier management approach ensures central control of applications and their license rules.

Enabling the Application Service Model

Service providers (SPs) combine software, hardware and network infrastructure to offer service-based applications to a large number of customers and their users. For customers, this enables them to concentrate on their core business processes while the SP provides infrastructure such as software license management, application hosting, billing, subscription management, service level monitoring, network delivery of applications, version management, help desk, consulting, and integration services.

Today there are three predominant SP models:

- *Co-locating* – application servers are co-located with a bandwidth provider (ISP). The SP manages application servers, integrates and customizes the offerings into the customer's existing infrastructure.
- *Dedicated* – the outsourcing model in which the SP provides dedicated machines to a business running a fixed set of applications. The SP manages both application content and infrastructure and provides a guaranteed level of service and availability.
- *Shared hosting model* – the SP provides bandwidth, machines, and software services for supporting shared applications. The applications are shared among multiple enterprises with multiple users on a virtual host.

Among these, the shared hosting model clearly provides the greatest potential for economies of scale and therefore a lower incremental cost for each customer. Shared hosting can either be **closed**, offering a specific set of applications to each customer, or **open**, where the customers and users themselves can subscribe and install applications that are delivered by the SP.

A shared hosting model is challenging to implement. It must accommodate rapid change and constant flux where new applications, subscribing companies and users must be constantly added. The SP must support multiple operating systems and versions of applications to provided a comprehensive solution. Service level agreements (SLAs) must be delivered and managed, and multi-tier application architectures supported. In this very challenging environment, the SP must strike a balance between their costs of operation and the levels of service they provide to customers.

7M Aspire is designed to support a shared hosting model. With 7M Aspire, the hosting model can be deployed internally in large organizations, but also with SPs as a means of managing the complexity of application and user provisioning. The flexible licensing models, delegated (self-service) user management and central control over applications enable the simple management of a large number of users, applications and customers. Centralized usage metering allows flexible integration with third party billing and SLA tools.

For customers that are not yet ready for the shared hosting model, 7M Aspire also provides the ultimate transitional solution. By implementing 7M Aspire inside the company firewall, security can be ensured. This can be done in a dedicated hosting model, where the actual management of applications and infrastructure could be outsourced. A company can thus implement the hosting model immediately. By

leveraging the distributed capabilities of 7M Aspire, the solution could then be gradually expanded to also include applications that are hosted externally, i.e. a combined dedicated and shared hosting model.

Flexible Administration

The core unit in a 7M solution is a 7M Aspire server. A configuration could consist of a single or multiple servers. Each server is a software unit, meaning that one single hardware server could host multiple 7M servers, or a single 7M Aspire server could be distributed across several physical servers in a clustered solution. Our use of "server" in this paper refers to the logical software unit.

7M Aspire servers span by default one *domain*, which is the administrative unit. A single domain server is a self-contained unit, capable of managing applications, licenses and profiles for a defined user community.

Administrators on a domain server can create multiple new domains or administrative units. A domain typically contains a group of users with their associated application profiles and usage data. Domains are organized hierarchically, thus a single domain could contain 10,000 users or it could contain 100 domains with 100 users each. Such administrative sub-domains could be departments or business units internal to the organization, external groups such as business partners or customers, or in a shared hosting model each domain could be a separate customer organization altogether.

Secure Administration

The main purpose of such domains is to assign administrative roles and privileges in a flexible manner. In 7M Aspire, each domain can be assigned a set of administrators. The administrator is then given one or more roles, e.g. User Administrator, Profile Administrator, or License Administrator. Each role gives access to a defined set of actions upon the domain. For any given domain, one person could have several administrative roles or a single role could be delegated to several users. Users could also have administrative roles in multiple domains.

This administrative security model is implemented in two levels. On the one hand, when an administrator loads the 7M Aspire management module, only the set of domains and operations on these that are defined by the given roles are available. Secondly, each operation is verified on the server side to ensure that the current user is authorized to the given roles.

This fine-grained administrative model is simple to manage, yet offers unprecedented flexibility. Administrative roles can be delegated to bring user profile management as close to the end users as desired without compromising existing security policies. In a hosted model, application and license management can be centralized whereas user management is delegated to the customers' own local IT departments or HR functions.

Distributed Management

In the previous section, we described how a given 7M Aspire server could be subdivided into multiple domains for administrative flexibility. This single server can be clustered in order to support a large number of domains and users from one central location. In addition, it could be useful to distribute functionality across several separate 7M Aspire servers:

- Geographical distribution – with low bandwidth connections between different locations, performance gains can be achieved by placing servers closer to end users
- Functional distribution – whereas separate business units or organizations may host and/or manage their own applications inside their firewall, certain applications could be provided from other SPs.

In these cases, the challenge is to avoid several different management systems, which would seriously impair the potential productivity and cost gains.

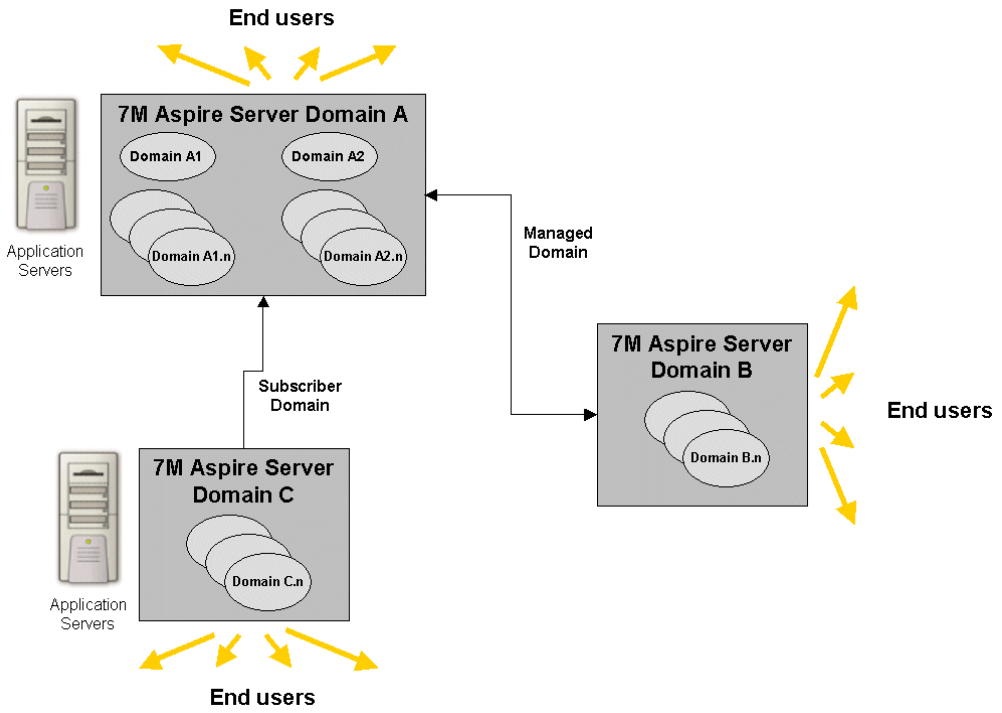

Figure 2. Multiple Administrative Domains.

Configuration Scenarios

Figure 2 illustrates how these scenarios could be addressed through 7M Aspire. Three servers are shown with primary domains A, B and C. 7M Aspire allows administrators to establish "*trust relationships*" between such servers. In this diagram a "*Managed Domain*" relation is defined between A and B, and a "*Subscriber Domain*" relation between A and C. A is a standalone domain server, managing a set of local application servers and users.

B is a domain server without its own applications; all applications are managed from server A. B could be a satellite office in a large organization, or a separate customer to a shared hosting SP. B could be separated due to bandwidth reasons, or for security purposes where all user and profile information is stored separately from other SP customers.

Server C is a standalone 7M Aspire domain server, managing a set of users and local application servers. In addition, C subscribes to certain services or applications from the central provider A. C could be managed within a local IT department in a large organization, or it could be a customer to a shared hosting SP where only certain applications are outsourced.

These scenarios further illustrate the flexibility of the 7M Aspire solution. An administrator on server A can be given specific administrative privileges on domains hosted on other servers, such as B. This administrator can manage functions on distributed servers from a single management console within well-defined security

bounds. The owners of server C can securely manage their own server, yet subscribe to external applications and manage these within the same administration framework, without changing systems or user interfaces.

For SPs, 7M Aspire also enables an aggregate hosting model. A central hosting center can provision, manage and distribute applications from a single source. Several SPs can subscribe to services from the central hosting center, controlling licenses and their own customers (individual domains). Each individual customer of these SPs can again add their own users and manage their application profiles, or the SP can perform this service for smaller organizations. The flexibility provided by fine-grained administrative roles and distributed server management allows for the tailoring of the solution through simple configuration tools without compromising overall security and control.

Architecture

The core architectural design requirements for 7M Aspire have been:

- Robustness and scalability: ensuring the secure and stable handling of a large number of users and applications;
- Standards based: the consistent use of open standards to integrate seamlessly with existing application infrastructures;
- Flexibility in configuration: using a modular and component based approach that facilitates the easy tailoring of a solution according to individual needs;
- Platform independence: designing for portability between application servers in order to minimize dependencies on individual third party vendors.

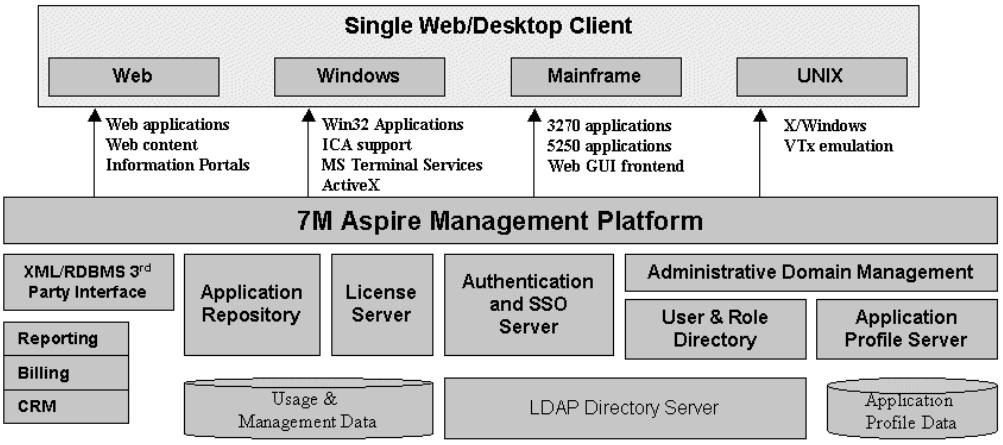

Figure 3. 7M Aspire Architectural Overview.

Overview

7M Aspire is designed on a multi-tiered service layer model. The different tiers communicate using standard protocols. A specific implementation of 7M Aspire is typically distributed across several physical and/or logical servers. This approach enables an organization to tailor their configuration for optimal performance, cost and security requirements.

A layered architecture better encapsulates the actual implementation of the different tiers. This reduces the dependencies among modules to well-defined interfaces and simplifies change when different tiers are implemented on several programming platforms.

The business logic is embedded in different components that execute on the server side. This logic is implemented using Java 2 Enterprise Edition (J2EE) and runs on a standards-compliant application server, e.g. IBM Websphere or BEA WebLogic, that provides high-performance, robust transaction and security support.

7M Aspire is based on a set of industry standards:

- J2EE for server side business logic

- HTTP for client-server communication, RMI/IIOP between servers
- XML for data exchange and external communications
- LDAP/X.509 for user authentication
- JDBC for database connectivity

The thin, browser based client approach not only allows users to run the applications from anywhere on a network, but also enables the integration and customization of 7M functionality into different existing client environments. End users can either use the standard 7M browser client, or access this functionality from an existing portal or even native client environment.

Application Repository

The application repository is the central storage and access point for applications in the system. Using administrative tools, existing applications are registered into 7M Aspire. The information in the store is normally a reference to an application residing on an existing application server, where the reference data vary according to the application type. However, this does not entail reinstalling or modifying existing applications.

During runtime, a client will load this reference information indirectly via the authentication and license control subsystems. Clients cannot bypass these security layers, ensuring that there is no backdoor to the real applications if normal system security routines are followed.

Application reference information is stored in a relational database backend. This store handles versioning to accommodate application upgrades and potentially the simultaneous management of different versions of the same application. The system administrator can also securely install and distribute new administrative applications to different 7M administrators.

The repository also has the capability of hosting web applications, for example a Java or HTML based terminal emulator. In this case, all necessary resources can be registered and uploaded to this repository, which will then act as the web server container for such applications.

Access to the application repository is also available via XML based command line utilities for automated provisioning.

The following types of applications can be managed from the application repository:

- *Web applications*. These can be hosted either in the 7M Aspire server, or on any other web server including IIS, Apache or Netscape. Web applications can be HTML, Java or Microsoft ActiveX based front ends. In the case of Java applets, the sandbox security policies are managed in the application repository, as are any applet parameters.
- *Windows applications*. These are normally executing on a Microsoft NT/2000 Terminal Server and can be delivered using different emulation technologies. 7M Aspire has built-in support for Citrix Metaframe and can run the applications as ICA clients with full integration for user authentication and server farms. Alternatively, other emulation tools can be used such as Microsoft Terminal Services Advanced Client, HOBLink JWT, etc.

- *UNIX applications*. 7M Aspire supports both terminal emulation and X Windows applications running across the web.
- *Mainframe applications*. 7M Aspire has support for VT, 3270 and 5250 emulation from a mainframe application server to the portal front end. Web based front-ends to terminal sessions through "Green2Web" screen scraping tools are also available. Existing terminal emulators from vendors such as IBM, WRQ, etc. can also be plugged into 7M Aspire.

7M Aspire has thus been designed for openness and flexibility in plugging in different emulation software. This ensures that the users are not locked into a specific vendor solution, but can select the best of breed tools to configure the optimal application portal from both performance and cost perspectives.

The application repository also includes a runtime subsystem. The purpose behind this is primarily authentication, to ensure that users that access applications are indeed authorized through the appropriate channels. Secondly, the runtime system is also used to modify application parameters dynamically, once the user, device and location have been identified. Application descriptors are generated XML documents that can be modified through a series of filters upon a user request. For example, a request for an application from a Citrix server farm can automatically be routed to the farm geographically closest to the end user before it is delivered to the client. Similarly, application parameters can be determined from the device in use to deliver custom application interfaces to users accessing the application from e.g. a mobile device.

License Server

The license server is responsible for application provisioning, license control and usage monitoring in 7M Aspire. It thus contains both administrative and runtime subsystems.

From the administrative point of view, the license server manages the association between applications and licenses. Applications that are available in the application repository can be associated with a license for a specific domain. The license contains information about the application, the license model, constraints, cost information, and the recipient of the license. Recipients could be all or a specific set of domains.

7M Aspire currently supports a set of different license models. Each model is associated with a set of constraints, typically time and number of users. For example, a concurrent license could be valid for a given period of time (1 year) and for up to 1,000 concurrent users.

The following license models are supported in 7M Aspire:

- *Demo*: A free license for test or evaluation purposes.
- *Concurrent*: Based on a finite number of concurrent users. The cost is fixed, and typically based on the upper limit of concurrent users that are guaranteed access.
- *Lease (Named users)*: Based on a finite number of total users. Unlike the concurrent model, all the users would be guaranteed access at all times. The cost is fixed, typically based on the upper limit of users that are guaranteed access.

- *Pay Per Use*: No specific user limits, although a maximum limit of concurrent users can be specified. The cost is variable, based on the number of times that the application has been accessed.
- *Unlimited*: Similar to a lease, but the number of users is unlimited. The cost is fixed.

Cost information is also associated with a given license, indicating how this service is priced. The cost information varies according to the license model. For a concurrent license, for example, the cost would typically be determined from the combination of a flat rate and a cost per concurrent user.

Licenses are associated with given domains (departments, organizations or customers) that subscribe to a given application. The runtime license system will perform license control to automatically verify and issue licenses to individual users before they are allowed to access the application. Upon completion or after a defined idle period, licenses are then revoked and released back to the pool. Usage information is logged to a relational database repository for reporting purposes.

Using the license administration console, authorized users can quickly and easily complete application provisioning by defining any number of license packages with defined user limits and possibly also with associated costs. This information can be updated at any time and ensures complete central control of license usage and cost tracking.

Examples of reports that can be generated from the 7M Aspire server include:

- Usage data for individual users, projects, departments or entire organizations that are fed into a billing system. This enables a service based hosting model either internally in an enterprise or across multiple customers.
- Usage data for monitoring license utilization, highlighting areas where license costs can be reduced or where too few licenses are issued.
- SLA statistics such as response times, refusal of service, etc.

Reports can be produced directly from SQL data or via intermediate XML data files.

User Authentication

7M Aspire is a gateway to disparate applications and information systems. Most of these are designed to manage their own authentication and use different management schemes to verify a user's identity and determine access privileges within that application or system.

For end users, the reality is therefore often that multiple logons and passwords are required to carry out normal business tasks. This is typically a significant source of helpdesk queries in many organizations. For IT departments, a large portion of time and resources may be spent on user management across many different directories with different administrative tools.

7M Aspire requires that users be authenticated when entering their application desktop. However, the approach to user authentication offers a full integration with the existing security infrastructure of an organization. Thus, 7M Aspire does not introduce a new level of user management for IT administrators. 7M is designed for pluggable authentication modules that integrate with most normal user databases today. Based on the Lightweight Directory Access Protocol (LDAP), 7M Aspire will

search for users in existing LDAP-compliant directories that are configured by the administrator. This eliminates the need for additional user management. For example, 7M Aspire will plug directly into directories from vendors such as Novell, Sun/Netscape, IBM and Microsoft.

Authentication is thus always passed on to the designated directory server. For a larger organization separated into several administrative domains, different domains can connect to different directory servers for authentication. 7M Aspire therefore is well suited for a real world directory infrastructure, where larger or distributed organizations may contain several disparate directories.

Authentication is today normally password based, encrypted using SSL. However, 7M Aspire will also offer integration with Kerberos or Public Key Infrastructure (PKI) authentication. Kerberos offers the advantage of integration with existing network single sign-on infrastructures where these are being used. PKI authentication offers greater security through secure data encryption and integration with a digital certificate authority. PKI also enables the use of external authentication mechanisms such as smart cards or biometric systems.

SSO Server

To address the problems of multiple logons to different applications, 7M Aspire offers a single sign-on (SSO) module that allows enterprise network users to seamlessly access all authorized network resources on the basis of a single authentication. This is an optional module that can be added on to 7M Aspire in a controlled manner.

The purpose of SSO is to allow users to log on once to the desktop. When a user loads disparate applications requiring separate authentication, possibly with different user names and passwords, 7M Aspire enables the automatic authentication against this application. The advantage is that users do not have to remember multiple logon names and passwords, simplifying the end user experience and reducing the need for support and central management, while maintaining security requirements.

SSO is an optional feature in Aspire that can be configured per application and user groups. Potentially, users could run some application with automatic SSO and other applications where security needs require separate authentication each time the user accesses the application.

7M SSO is designed for simple administration, security and maximum user self-management. It consists of a server side repository that stores account information per user and application, encrypted in a relational database. This information is only available to the individual user. When a user loads an application for the first time, login panels are intercepted to record the authentication information (user name and password). This information may be captured on the client side or on a server, depending on the type of application and authentication protocol. The logon credentials are encrypted using SSL and transferred to the authentication server for storage and future reference. This procedure is repeated if the user is prompted for new credentials at a later stage (e.g. expiring passwords).

The next time the user loads this application; the authentication server will have issued a ticket to the user. This ticket is used to retrieve the account information for that application, encrypt this information using SSL, and passing it through to the application authentication front end.

The 7M Aspire logon can also be integrated with existing authentication mechanisms. This is useful when the application portal functionality of Aspire is embedded in a

different end user client such as an enterprise information portal.

Robust, scalable application platform

7M Aspire is designed for deployment in large organizations with many users, even if they are distributed geographically. The application platform provides the scalability to handle these requirements. This entails performance issues related to network traffic, application sharing, session management, and database connection pooling and caching. The ability to run the total solution in a load-balanced cluster of computers promotes scalability.

The architectural design also improves the stability of a solution because having applications run across a network and a multitude of client and server platforms was integral to its development. There are many potential points of failure in such a solution, and the application framework is designed for robustness and to detect and handle anomalies.

7M Aspire is designed to avoid the use of proprietary clustering and load balancing solutions. Rather, standard clustering hardware and software can be used to enable the required scalability and fail-over capabilities of an enterprise application portal.

One central purpose of the application deployment portal is to deliver applications securely to the end user with minimum runtime overhead. The application is initially accessed through the license and application runtime systems, in order to verify authorization and enforce usage control. Once the application is loaded from the backend application server, however, the user will be directly connected to this service without incurring any intermediary overheads.

7M products enforce strict quality guidelines. This also include error handling and event logging, ensuring that any error situations that may occur will be handled as gracefully as possible, and that event logs are being generated. Event logs also include security issues such as refused authentication, etc. These event logs can also be provided to third party system management tools, such as CA Unicenter TNG or Tivoli. This ensures that the status of the system can be monitored using standard tools and methodologies.

The end user client

End users access their application portal from a secure HTML client. The client is accessible on a LAN, WAN or across the Internet. The user logs on from a web page in a browser. No client side administration is needed. Data encryption between a client and the domain server is done through SSL across an open connection

To simplify third party integration, the user profile that is used to generate the portal desktop is available as a generated XML stream. All runtime communication between the client and the license/application runtime systems is also done in XML. It is therefore easy to embed the application profile into an existing client side application, including browser based information portals or native desktop front ends.

The HTML client is designed to be either a standalone desktop running in a browser window, or a part of an existing web front end. The look and feel of the HTML client is completely configurable through the use of standard style sheets. These style sheets can be chained transformations that deliver a custom GUI based on the end user, the domain, the geographic location, client side language settings, and the actual device from which the user is logging in. 7M Aspire offers a framework in which these style sheets can be easily plugged in and executed to create a corporate brand.

The 7M Aspire application portal acts as the gateway between the client and all legacy data and applications. Users are given a single point of access for their

organization's internal and external information resources and applications, regardless of platform, technology or database. Through this gateway, access is provided to applications running on servers such as Windows 2003/2000/NT Terminal Servers, Unix or mainframes. In addition, 7M Aspire provides access to Java applications and HTML based business portals. The applications can be a mix comprised of those served up by one or more service providers and internally installed applications. One common, intuitive user interface makes it easy for users to navigate through large masses of information and quickly retrieve relevant data.

The majority of clients today are based on various Microsoft Windows operating systems. For these users, 7M Aspire provides specifically integrated functionality with the user's desktop and with the Internet Explorer browser.

Growing the Solution

7M Aspire jumpstarts the application portal by rapidly web-enabling existing legacy applications. The modular design allows you to start in the small with a limited number of users to establish a pilot solution. This stage typically involves the migration of existing applications to a server centric model, end user portal integration, and establishing the security and administrative infrastructure.

The solution can then be rapidly expanded in a controlled fashion by adding new modules and rolling the application portal out to a growing number of users. The immediate benefits are now reaped through increased end user productivity, reduced support overhead and lower overall cost of ownership. An application deployment infrastructure is now established that will grow with the business and adjust to changing requirements.

The next steps typically involve the integration of new web components that communicate with the existing legacy backends. Current or planned portal or Enterprise Application Integration efforts can be coordinated within an administrative framework where new applications can be deployed in a stepwise fashion. This approach buffers change processes and minimizes risks involved in the introduction of future IT solutions.

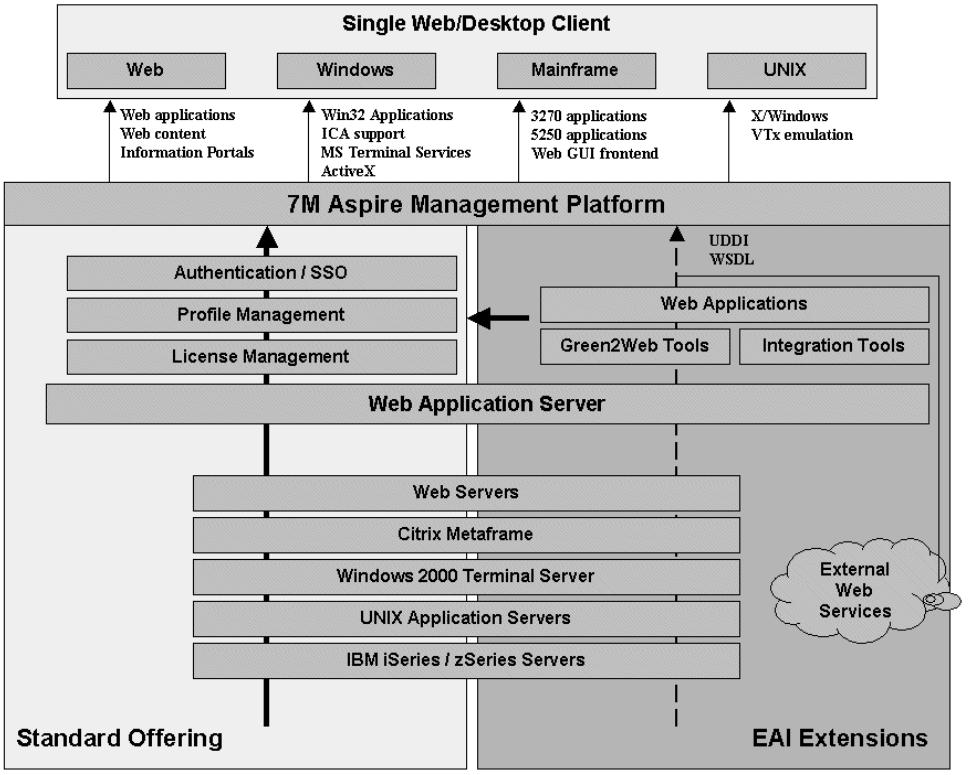

Figure 4. Extending the 7M management framework to include new application infrastructures

Summary

7M Aspire offers an application deployment portal that gives immediate structure and value to an IT environment. The solution encompasses the needs of end users, IT administrators and financial executives. The benefactors typically are:

- Organizations with a large and/or highly distributed and mobile user community
- Organizations with a complex and heterogeneous IT infrastructure
- Service providers offering a shared or aggregate hosting model to many customers with individual needs
- Software vendors who want to develop new business models by offering their software as services to a broad user community
- System integrators that provide integration services to multiple customers

Simple, yet sophisticated management solutions combine the central control of critical resources with high agility in responding to the changing needs of a large user community. Turnkey components help reducing the implementation time and cost and allow the controlled introduction of a server centric application model.

A foundation in open standards and a robust, scalable infrastructure ensures that the management solution can be integrated with and enhance existing e-business strategies. Agility in integration increases your ability to manage the future.

Contact Information

Seven Mountains Solutions AS
P.O. Box 1034
5808 Bergen, Norway
Tel: +47 55 70 64 10

www.7m.com