



# ATOMA™

## Technical Overview

### White Paper

---

#### **Abstract**

This paper provides information technology professionals a technical overview of the features available in Abaco's ATOMA framework. The framework provides a scalable architecture for development, deployment and management of enterprise mobile applications.

© 2001 Abaco, Inc. (Abaco) All rights reserved.

*The information contained in this document represents the current view of Abaco Mobile on the issues discussed as of the date of publication. Because Abaco Mobile must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Abaco, and Abaco cannot guarantee the accuracy of any information presented after the date of publication.*

*This white paper is for informational purposes only. ABACO MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.*

*Other product and company names mentioned herein may be the trademarks of their respective owners.*

Abaco • 1100 Northmeadow Pkwy, Suite 150 • Roswell, GA 30076-4960 • USA  
2001

---

## CONTENTS

|                                  |    |
|----------------------------------|----|
| INTRODUCTION .....               | 1  |
| Architecture Brief .....         | 1  |
| SETUP AND DEPLOYMENT .....       | 3  |
| CONSOLE.....                     | 4  |
| User Management .....            | 4  |
| Monitoring & Configuration ..... | 4  |
| Security Administration .....    | 4  |
| Application Management .....     | 4  |
| USER AUTHENTICATION.....         | 6  |
| SECURE AUTHENTICATION .....      | 7  |
| DATA PIPING .....                | 8  |
| TX SYNC .....                    | 10 |
| DEVICE FRAMEWORK.....            | 12 |
| CONCLUSION .....                 | 13 |
| ADDITIONAL RESOURCES .....       | 14 |



---

## INTRODUCTION

Nobody likes to sit still. As enterprises reach for greater efficiencies in all areas of operation the general consensus is that in order to achieve improved efficiency each arm of the enterprise must make the best use of time.

Consider a beverage sales representative who visits customers on a daily route. This representative creates orders for products as requested by each customer, keeps notes regarding sales trends as information is gathered from each customer, and gives information regarding promotions and new products to each customer. How does the sales rep keep informed of new promotions offered by the beverage company? When placing an order how does the rep provide accurate feedback as to when the order will be shipped, print invoices, scan products that require reorders to speed information gathering and ensure accuracy? How can the rep automatically read information collected in vending machines that are on the sales route?

Now lets examine the requirements of a solution for the beverage sales representative's real enterprise needs:

- There are 5000 sales representatives working on routes and the beverage company will not depend on one device vendor so the application must support multiple device brands.
- The sales representatives perform most of their duties off-site, in areas where network coverage is not available.
- The orders created by the sales representatives must use information stored in enterprise information systems and must be created while applying centralized business rules established for sales orders. These business rules have already been implemented using a number of disparate technologies including CORBA, EJB's and COM+.
- Due to an ultra competitive environment between beverage companies the system must ensure that communications containing sales information are secured and that only authorized sales representatives are able to access the application and corporate resources.

In order for the beverage company to be successful in delivering this solution, the resources at the beverage company must be able to focus on their core competencies: the business rules of the company and the application functionality required. In order for the solution to be able to grow with the growing needs of the company and it's employees, the solution must take advantage of open protocols and standards to ensure its longevity.

To achieve enterprise goals and to meet system requirements such as the ones outlined above and those that may come in the future a robust and open mobile architecture is needed and that architecture is ATOMA.

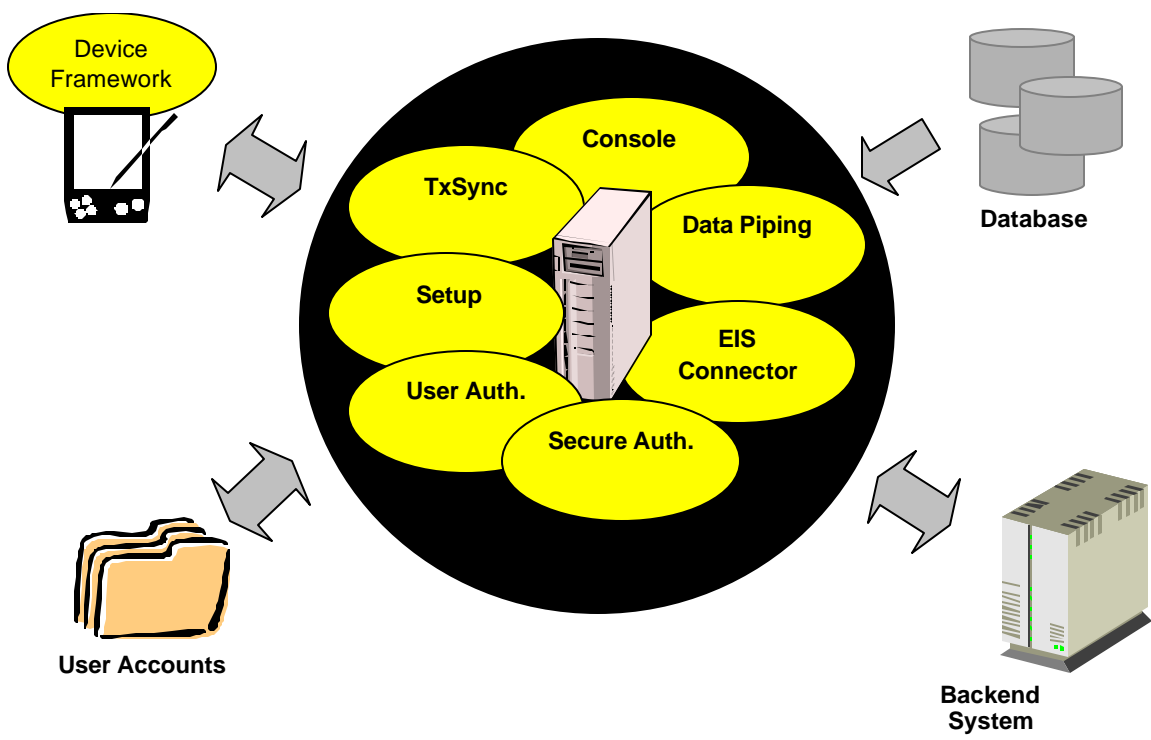
### Architecture Brief

The ATOMA architecture is designed to support large numbers of mobile devices, provide services independent of the operating system and platform and provide speed

and efficient usage of the limited resources found in mobile devices. The server-side architecture is based in J2EE, works in concert with any application server on the market and allows the use of any programming object model for logic encapsulation and business rule reuse.

The client-side architecture is based in the native languages supported by the device operating systems to achieve a small memory footprint, efficient power consumption, and ability to interface with any peripheral supported by the device.

Figure 1: XOOM Architecture



## SETUP AND DEPLOYMENT

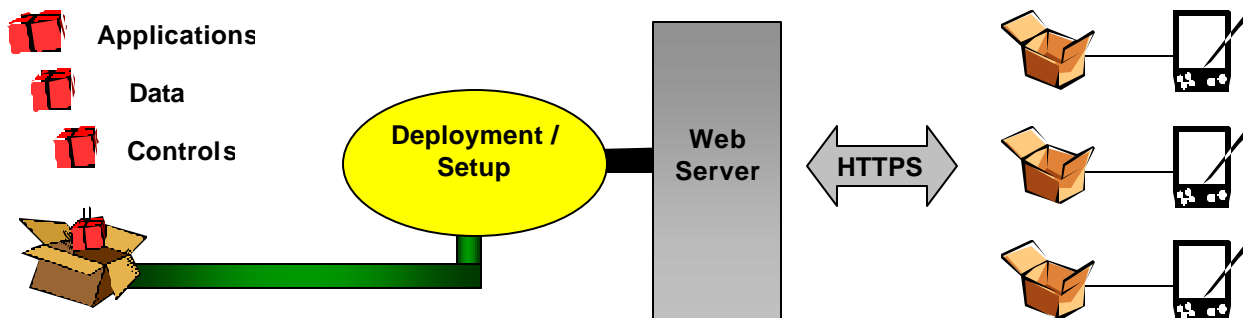
One of the primary goals of the ATOMA framework is to streamline the process of initializing and configuring mobile devices. The setup and configuration of devices is typically the most mundane time consuming and costly process associated with the management of a mobile system. Due to the volatile nature of embedded device usable memory, the setup and configuration cycle is typically repeated each time the device battery is discharged or the device reverts back to factory settings because of a reset operation or condition. By automating the setup process, the management of a mobile system is greatly simplified and significant cost savings are realized due to the reduction in human intervention necessary to initialize a device.

The mobile device setup process is primarily achieved through a browser. Using the web browser found on today's mobile devices, a user simply navigates to the HTTP URL associated with a ATOMA server. Once the user is authenticated, the device being used is automatically identified and the device framework components appropriate for the device are downloaded. These components are packaged in a compressed self-extracting module that installs the included components and performs a number of additional steps to complete the setup process. During these additional steps the applications assigned to the user are installed and the data and database structures for the user are downloaded to the device.

While most of today's mobile devices are equipped with a browser, settings for a network connection typically must be configured before the browser becomes useful. To overcome this obstacle, a Setup Card utility is provided where using compact flash and eventually Smart Cards, custom network configurations can be prepared and saved on a Setup Card. When inserted into the device this card automatically configures the connection settings of the device allowing the browser-based setup to proceed seamlessly.

ATOMA's automated device setup process provides an elegant and efficient solution to one of the more difficult problems facing any mobile device management system. The benefits of this automation include a drastic reduction in the time required for device initialization and a corresponding increase in the overall user-friendliness and availability of the system

Figure 2 Setup process



---

## CONSOLE

A key feature of the ATOMA system is the capability to centrally manage an entire network of client devices and to also manage a ATOMA installation from the same environment. These capabilities are provided by the ATOMA Console - a web based application which empowers a system administrator to remotely configure and monitor client devices and also manage server-side settings and configuration options.

### User Management

The Console avoids the administrative nightmare of creating and managing multiple user databases by seamlessly integrating with user management systems already in use by an enterprise. After specifying an LDAP\* compliant repository where user accounts are stored, the Console can be used to organize imported users into groups.

\*Microsoft Windows NT Security Accounts Manager also supported

### Monitoring & Configuration

As users synchronize using ATOMA's patent pending technologies in the TxSync process, information describing the status and settings of a device are reported to a server. This information can be viewed for any device at any time through the Console allowing system administrators to monitor the devices to establish user trends and to preempt device related issues. The Console also enables configuration of client devices where the applied settings are realized during the TxSync process. Through device configuration, system administrators can take control of numerous settings on the client device such as power management settings, network connection settings, device display settings, and much more.

### Security Administration

Coupled with the framework's support for Secure Sockets Layer and 128-Bit Encryption, a complete Certificate Authority is provided to enable issue and revocation of Digital Client Certificates to system users. The settings for this Certificate Authority and the settings for Digital Client Authentication are all managed through the Console.

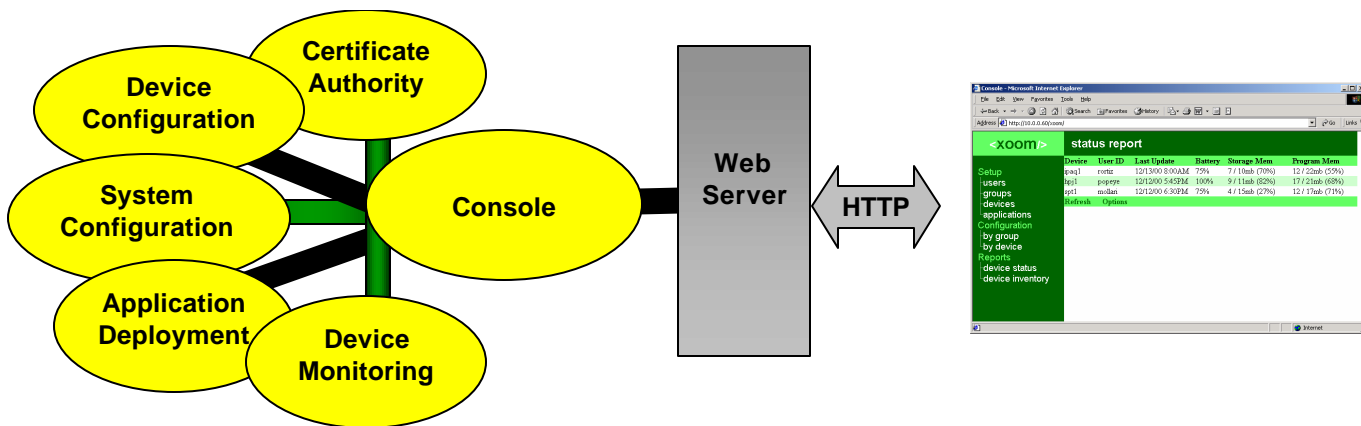
### Application Management

ATOMA application can take on many forms: an executable, a set of HTML forms and pages combined with scripting technologies. Regardless of the form an application takes, it is ultimately delivered to an enterprise user's device to allow that user to perform his or her daily tasks. Using the Console administrators and developers can centrally deploy applications to all users of the ATOMA system. Applications can be assigned to groups of users (as defined above in User Management). Updated versions of applications can also be deployed such that the application will be updated on all devices having different versions.

The Console is the central administration and configuration tool for all ATOMA modules and processes. Due to the adaptability of the ATOMA framework, there are several options and settings that can be used to customize the framework for distinct enterprise computing environments. The Console consolidates the myriad of options and tools into

a manageable, user-friendly web application.

Figure 3 Console



## USER AUTHENTICATION

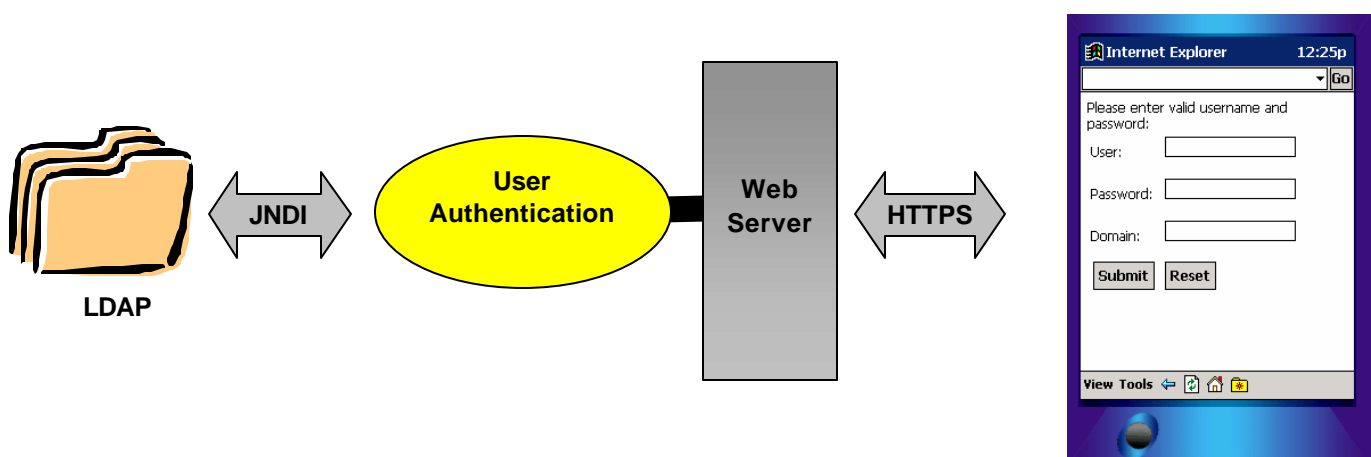
User Authentication is the process of verifying the credentials of individuals who try to access a system's resources. User authentication provides the basic foundation for any secure software or networking system. There are several excellent systems in use today for the management of user accounts and the storage of user related information. Instead of duplicating the services provided by enterprise class user account management systems and causing system administrators to have to maintain duplicate data in separate user repositories, the ATOMA framework allows you to take advantage of the capabilities provided by an existing user management system by reading and validating any user related information against such an existing repository.

The ATOMA framework will interface with any LDAP compliant user account system and also includes support for the Microsoft Windows™ NT based security and accounts management systems. This interface occurs on two levels. First, in order to successfully administer a ATOMA system, information about the users of the client devices in the system is required. This information is always pulled automatically from a designated master user account repository alleviating an administrator from having to create and manage users separately for the ATOMA system.

The second level of interaction between a ATOMA system and an enterprise user account system is at the time of validation of a user's credentials. User credentials are always validated by the enterprise user account management system. Any time that a user logon of some sort is required by the system, the validation of the user's credentials is performed by the master user account system. By adhering to this model, ATOMA ensures that user information remains truly centralized and avoids several possible security weaknesses that might be introduced when user information, such as passwords, is duplicated in multiple systems.

The ATOMA system's use of User Authentication ensures that access to any enterprise resources available through the system is only granted after the requesting party's credentials have been centrally authorized. Tight integration with existing user account management systems ensures that administrators do not duplicate user management efforts and that users do not need to keep track of yet another username and password combination.

Figure 4 User Authentication



## SECURE AUTHENTICATION

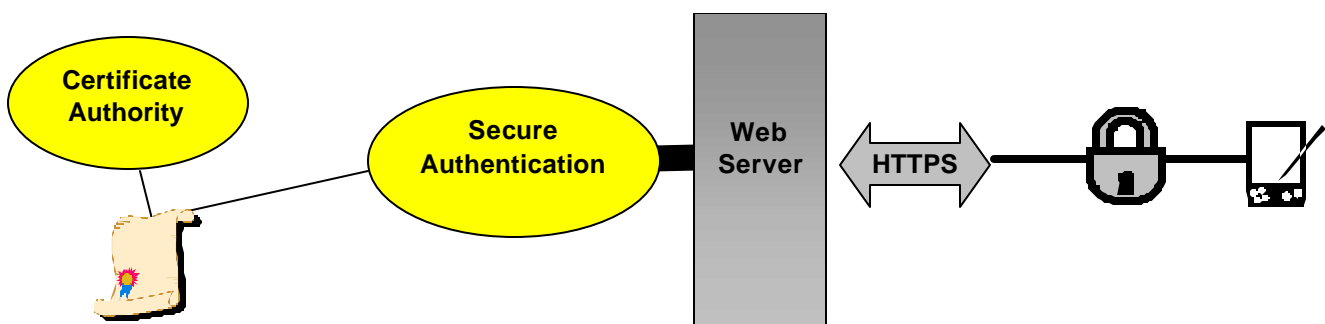
Secure Authentication is the process by which users requesting server services are granted or denied access during an otherwise secure communication exchange. Communications exchanged between device and server can be secured with 128-bit encryption using Secure Sockets Layer (SSL) and Digital Server Certificates. Secure Authentication adds Digital Client Certificates to these technologies to add verification of the identity of the party requesting a server's services and resources before granting access to those services and resources.

The ATOMA system's implementation of Secure Authentication provides automatic assignment and deployment of digital certificates to users. Once a digital client certificate has been deployed to a user it is no longer necessary to prompt the user for logon credentials to validate his or her identity. The ATOMA Device Framework takes care of presenting the user's client certificate when secure authentication is requested allowing the server to positively identify the user before granting access to a requested resource.

A number of server-side services are provided to support the Secure Authentication implementation. One such service is the Certificate Authority that manages the digital client certificates in use on the system. The Certificate Authority allows the creation and revocation of client certificates and provides a resource for validation of existing client certificates. An HTTP request filter is also provided to read certificates as they are submitted by client devices and to interface with the Certificate Authority to verify the validity of any given certificate.

Secure Authentication provides a way to digitally authenticate users to ensure that access to enterprise services is strictly regulated based on a user's credentials. The use of digital client certificates provides an added level of security to SSL communication exchanges that could otherwise possibly allow unauthorized use of enterprise resources.

Figure 5 Secure Authentication



Data Piping enables mobile users to receive individualized information to be stored locally on a client device.

The Data Piping process begins with the Data Piping Designer. This web-based tool allows application architects and developers to specify the data elements, originating from centralized enterprise data sources, which are required for their mobile application(s) and how these elements will be structured on the target device. These centralized enterprise data sources can be any combination of databases from the major database management system products in use today, such as DB2, Informix, Oracle, SQL Server and Sybase.

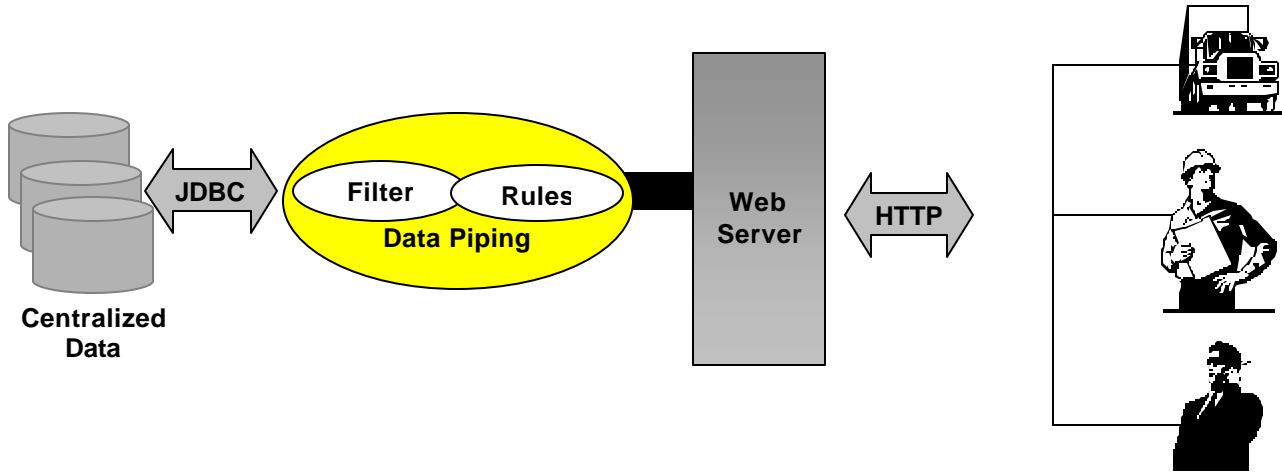
The Data Piping Designer essentially allows application designers to create application relevant subsets of the information stored centrally in an enterprise by graphically creating queries that can take into account specific user characteristics. While this functionality can solve many problems for an enterprise, ATOMA Data Piping allows an even further customization of the process. The system allows developers to supplement the queries created in the Designer with logic implemented in software objects to handle complex data dependencies and tasks that require processing which cannot be implemented through queries alone.

Data Piping is closely integrated with the TxSync process. During the TxSync process the data and data structures that are relevant to the user conducting the synchronization are delivered to the user's device in a platform independent XML-based format. This XML-based format allows freedom of choice to mix and match database management systems on the server with database systems on the device, allowing enterprises to select best of breed solutions instead of being tied to any single vendor.

The actual preparation of data and data structures for a specific user and piping instruction set can happen in one of two ways: by schedule and/or during synchronization. When preparation is set to occur by schedule, the data destined for a device user is extracted from the centralized data sources at a specified time (or times) on a regular cycle. When preparation occurs during synchronization, the queries to extract data and the accompanying logic are executed during the TxSync process to provide the ultimate in flexibility and to ensure that only the most up-to-date data available is transferred to the user's device.

ATOMA Data Piping provides an engine capable of providing enterprise users with local data stores for information access while disconnected from a network and keeping these local data stores up-to-date with ever-changing data in centralized enterprise data sources. Data piping allows developers to create and manage data structures, specify data associations and compliment these structures and associations with logic to provide an intelligent method of providing enterprise users with only the information they need, when it is needed.

Figure 6 Data Piping



Abaco's TxSync is a unique process by which disconnected devices enabled with the ATOMA Device Framework accomplish synchronization with enterprise network resources. The primary goals of the TxSync architecture are to provide a scalable mechanism for simultaneous synchronization of large numbers of mobile users and to provide a model for reporting information from a client device to an enterprise resource that ensures the integrity of the information transmitted.

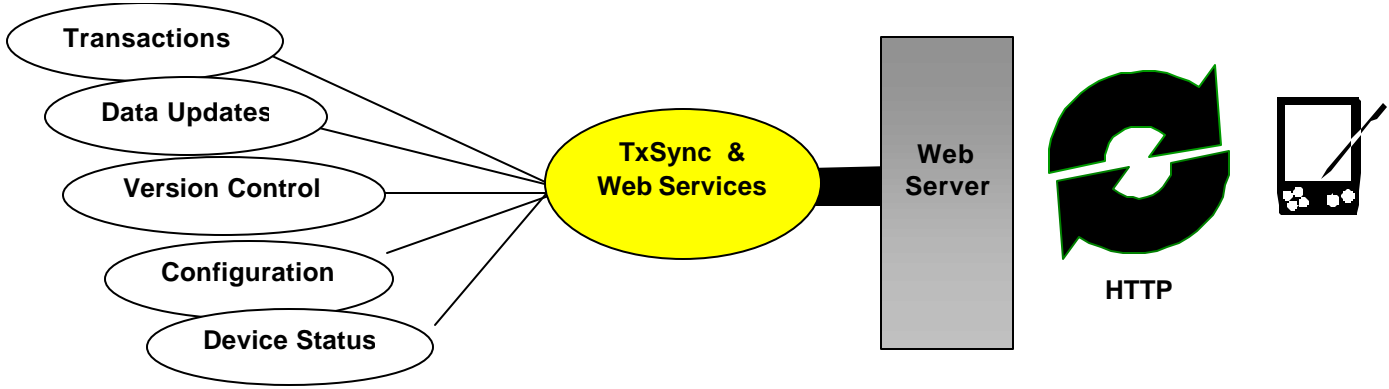
TxSync achieves its goals by combining SOAP (Simple Object Access Protocol) and a completely asynchronous architecture for maximum efficiency and reliability during the device synchronization process. TxSync adheres to the rules of fully self-contained transactions from the ground up. TxSync's fundamental concept is to use SOAP for all data traffic from the device to the enterprise resource. In this way the complexity, inherent pitfalls, and inevitable data collisions encountered in raw data synchronization or data replication systems is avoided. An added benefit of TxSync's use of SOAP for data uploads is that it allows enterprises to take control of data validation and processing rules without being tied to any single platform or system.

TxSync provides several features which ensure and protect the integrity of enterprise data as it is reported. Communications between the device and the TxSync server are completely asynchronous allowing straightforward recovery from inevitable breaks in network connectivity while the TxSync process is executing. The server modules of the TxSync system uniquely identify each synchronization to ensure that, in the case of a system error, data and calls to enterprise objects are not erroneously duplicated. The server modules also manage their state using non-volatile memory, such that in the case of a complete hardware failure, an in-process synchronization can resume where it was interrupted after a server is restarted.

During the TxSync process several tasks are completed in one robust operation: application transactions are reported to the server, changes to application database structures and data are prepared depending on the device-user and his organizational role, current status of the device is reported, version control of applications and system components is performed and system configuration changes are conveyed to the device. During the TxSync process potentially large sets of data are compressed to make best use of the available network connectivity and usage of the network is minimized by packaging needed information and data into single packages to eliminate the need for multiple calls and responses between the device and the server.

The TxSync process provides ATOMA systems with a fully integrated, robust mechanism for asynchronous information exchange between a client device and the enterprise network. The TxSync process enables mobile users to spend as much time as needed untethered to a network or operating in areas where coverage is not available with the assurance that the information created by their work will be reliably reported to their enterprise and their device will be kept up-to-date with the latest corporate information and settings applied by the system administrator.

Figure 7 TxSync



---

## DEVICE FRAMEWORK

The ATOMA device frameworks are designed to provide developers with a foundation to create robust enterprise applications. The fundamental services provided by a device framework are usage of web protocols for application communication, simplified and platform independent access to data capture peripherals, support for offline and online applications, efficient usage of device resources to conserve power usage, and automated application management, deployment and configuration.

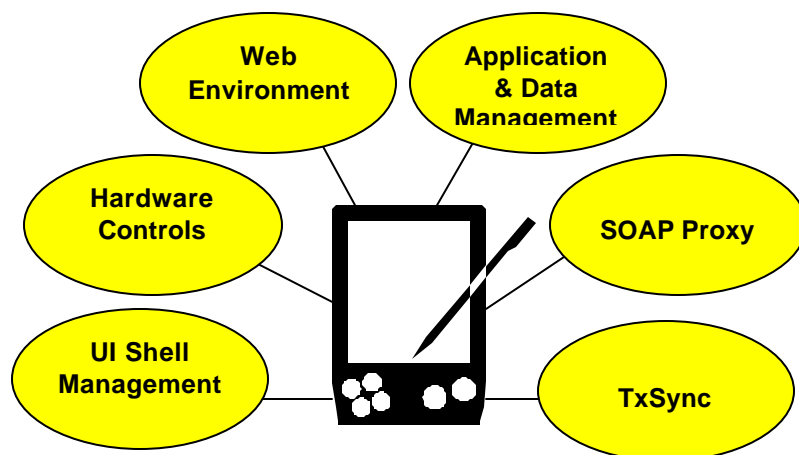
Each ATOMA device framework targets a particular operating system platform. Today ATOMA is delivered with the Windows CE device framework that targets Pocket PC and HPC 2000 devices. Future device frameworks will target Mobile Linux and Epcoc-32. For Windows CE, the device framework consists of a set of application programming controls, executable files, and supporting tools.

Device frameworks provide an application programming interface that supports embedded device application developed using web languages (HTML and ASP on CE), rapid application development languages (eMbedded VB on CE) and core supported languages (C/C++ on CE). Enterprises benefit from the device frameworks by reducing application development cycles, enjoying functionally rich applications, and having freedom of choice between different device manufacturers with minimal or no application portability issues.

The automated services provided by a ATOMA device framework present enterprises with an unparalleled opportunity to streamline operations and ensure that a mobile solution is operating efficiently and reliably. Many of these automated services are managed by the TxSync process to create the ultimate in flexibility between online and offline modes of operation. Services such as application version control, data piping, device configuration, and secure authentication give system administrators a level of control very rare in most mobile solutions.

To create a mobile application that has the capabilities required by Today's enterprises, two main ingredients are necessary: the correct mobile device for the target environment and a strong application development and management framework to support the desired application. The ATOMA device frameworks deliver on the second ingredient while allowing you to choose freely from any of the first ingredient available on the market today and tomorrow.

Figure 8 Device Framework



---

## CONCLUSION

Delivering a mobile solution is an inherently complex endeavor. While technological advances and the proliferation of new technologies have opened new possibilities, very few products have offered a cohesive solution to the requirements and desires of the mobile enterprise.

By delivering automated Setup and Deployment, enterprise User Authentication, Secure Authentication and communications, Transactional-based synchronization, complete system and application version control, remote device configuration and monitoring, and an intelligent data deployment architecture, ATOMA puts enterprises in a position to realize the goals outlined in a mobile strategy and to reap the resulting benefits.

---

## ADDITIONAL RESOURCES

Abaco Mobile Web site:

<http://www.abacomobile.com>

Java 2 Enterprise Edition Website:

<http://java.sun.com/j2ee/>.

Microsoft Pocket PC Web site:

[http:// www.microsoft.com/mobile/pocketpc/default.asp](http://www.microsoft.com/mobile/pocketpc/default.asp)