BlueStar: Wireless Claims Processing for the Property and Casualty Industry

D. Bantz, T. Buechner, T. Chefalas, D.J. Lan, G. Leonardi, L. Liu, S. Mastrianni, R. Moulic, D. Shea, J. Song. J. Song, A. Wyskida

***Abstract*—Mobile handheld devices communicating over wireless networks now represent a capable, robust, cost-effective, usable platform for enterprise mobile solutions. These solutions must be manageable, secure, scalable, and capable of integration with other enterprise components. The scale of mobile solution deployment demands high levels of automation to keep labor costs in check and to keep solutions running in compliance with enterprise standards for security and availability. This paper describes the design and deployment of a prototype wireless mobile solution for mobile claims processing for the Property and Casualty Insurance industry. We show how computer-based management processes and policies contribute to high levels of automation, making it possible for the large scale deployment of applications and services in the enterprise.**

***Index Terms*—Information services, Business communication, Productivity, Information technology, Information systems.**

I. Introduction

RECENT advances in the design and manufacture of mobile hardware have enabled handset manufacturers to provide a robust and powerful platform for the execution of enterprise-worthy applications. These devices now contain sufficient processing power and storage to handle even the most demanding corporate applications. Wireless carriers have continued to invest in their networks to provide higher bandwidth and improved data capability using technologies such as High Speed Downlink Packet Access (HSDPA).

The combination of small, powerful portable devices and increased bandwidth has enabled a new set of applications and services that can be leveraged by a large enterprise. One such application is that of mobile claims submission and processing for the Property and Casualty Insurance industry. This application places remote insurance adjusters in constant communication with the home office through email, messaging and shared calendaring facilities. It facilitates rapid tasking and dispatching of a damage claim, guides the adjuster to the site of a loss, records the necessary information concerning the loss including text, photos, recordings, signatures, and other required information, and sends that information back to the office for quick processing.

The ability to process claims quickly results in greater customer satisfaction and lower costs to settle claims.

Manuscript received May 1, 2008.

D. F. Bantz is with IBM Research, TJ Watson Research Center, Yorktown Heights, NY 10598 USA (email: dfbantz@us.ibm.com).

T. Buechner is with IBM Corporation, Global Insurance Industry, New York, NY 10010.

T. F. Chefalas is with IBM Research, TJ Watson Research Center, Yorktown Heights, NY 10598 USA (email: chefalas@us.ibm.com).

D. J. Lan is with IBM Research, China Research Lab, Beijing, People's Republic of China.

S. Jinho is with LG Corporation, Seoul, Republic of Korea.

G. Leonardi is with IBM Research, TJ Watson Research Center, Yorktown Heights, NY 10598 USA (email: leonardi@us.ibm.com).

L. Liu is with IBM Research, TJ Watson Research Center, Yorktown Heights, NY 10598 USA (email: leslieliu@us.ibm.com).

P. N. Liu is with IBM Research, China Research Lab, Beijing, People's Republic of China.

S. J. Mastrianni is with IBM Research, TJ Watson Research Center, Yorktown Heights, NY 10598 USA (email: stevemas@us.ibm.com).

R. Moulic is with IBM Research, TJ Watson Research Center, Yorktown Heights, NY 10598 USA (email: rmoulic@us.ibm.com).

D. Shea is with IBM Research, TJ Watson Research Center, Yorktown Heights, NY 10598 USA (email: dgshea@us.ibm.com).

J. Song is with LG Corporation, Seoul, Republic of Korea.

A. Wyskida is with IBM Research, TJ Watson Research Center, Yorktown Heights, NY 10598 USA (email: wyskida@us.ibm.com).

II. Background

A. Wireless Mobile Devices

When cellular phones were introduced to consumers in the mid 1980's, the average cost of a mobile phone was $1500.00. High monthly charges, substantial contract termination fees, and poor coverage initially slowed adoption. Today, advancements in semiconductor devices, packaging and communications technologies have driven the cost of cell phones below $100, and improved network coverage and capacities to the point where in 2006 cell phones were in use by over 71% of the U.S. population

Low-cost cell phones, increased bandwidth, flexible service plans, and the ability to always be in voice communication, have made cellular phones one of the fastest growing market segments of the telecommunications industry. For the first time in history, sales of mobile phones have eclipsed the sales of traditional personal computers. The use of mobile phones has become so pervasive in the consumer market that it's hard to find someone that doesn't use a cellular phone in some aspect of their life. Emerging markets in countries such as India and

China have experienced explosive growth in the adoption of mobile devices by consumers.

Applications, especially consumer applications, have been driven the market, prompting for innovations on both device and infrastructure. To differentiate their phones from each other, manufacturers bundle large suites of software applications such as music players, email clients, weather reports, traffic alerts, GPS navigation and access to maps. Some manufacturers are beginning to ship hardware and applications that allow the new phones to be used to buy merchandise, airline tickets, or to check in to hotels. In Japan, consumers can choose hardware which allows mobile devices to double as electronic wallets, which can be used for purchases at vending machines as well as many retail stores. More applications and features will appear as these devices become more powerful and network bandwidth increases. Because these devices are as powerful as some desktop systems, they can now be used to support the needs of the enterprise, as well as the consumer. Mobile devices now have the processing power, storage, and security required to support business applications, and now represent a capable platform for the deployment of many enterprise applications, such as creating-, manipulating and viewing office documents forms or spreadsheets, (see **Figure 1. Mobile Device Capabilities**)

Business, however, has been slow to adopt wireless mobile technology, due in large part to: 1) the high cost of deploying and supporting a large scale wireless, mobile infrastructure, 2) the challenges of maintaining existing enterprise security policies in mobile environments, and 3) the cost of transforming existing corporate business processes functions to a new wireless, mobile platform.

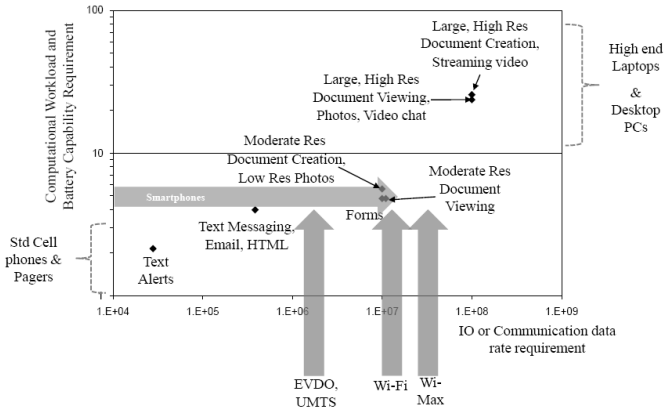

Figure 1. Mobile Device Capabilities

B. Mobile Systems Management

One of biggest challenges has been the ability to easily and cost effectively deploy and manage large numbers of mobile devices. Devices have to be provisioned, deployed, and managed throughout their life to insure that they meet the needs of the business, including the security of the device and the data it may contain, safety, and governance. Managing mobile devices has traditionally been labor intensive, driving some companies to move their support centers abroad to keep support costs down. Tools for managing mobile devices generally require some type of interaction by a support representative while the end user waits on the call.

Traditional management tools such as Nokia's Intellisync© Management Suite provide the ability to perform certain systems management functions for mobile devices. On Windows 2003 server, the Nokia tools are accessed and execute under the direction of an IT administrator through a Microsoft Management Console (MMC) plug-in. The plug-in provides a Windows-like graphical interface for performing certain systems management actions (see Figure 2. Nokia Intellisync Management Console).

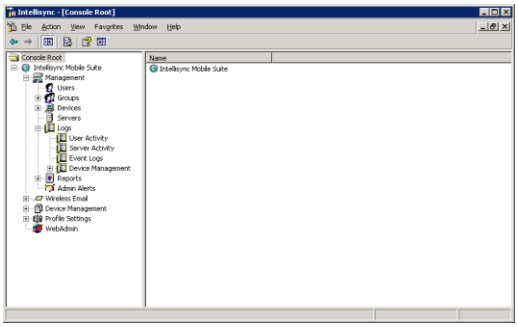

Figure 2. Nokia Intellisync Management Console

The Nokia Intellisync management console is accessed the same way as any traditional Windows application with a few minor exceptions. The administrator logs onto the Windows 2003 server, runs the Intellisync administrator plug-in, and selects the systems management functions to perform.

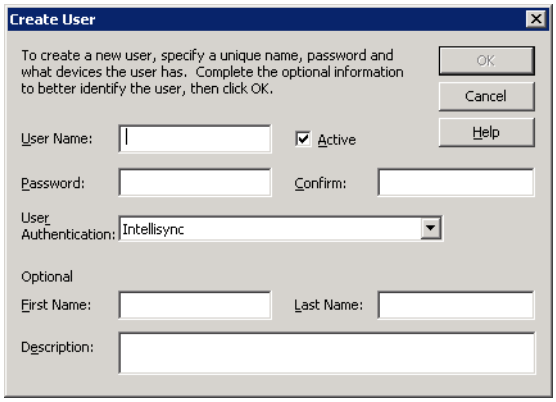

Figure 3. Adding a user

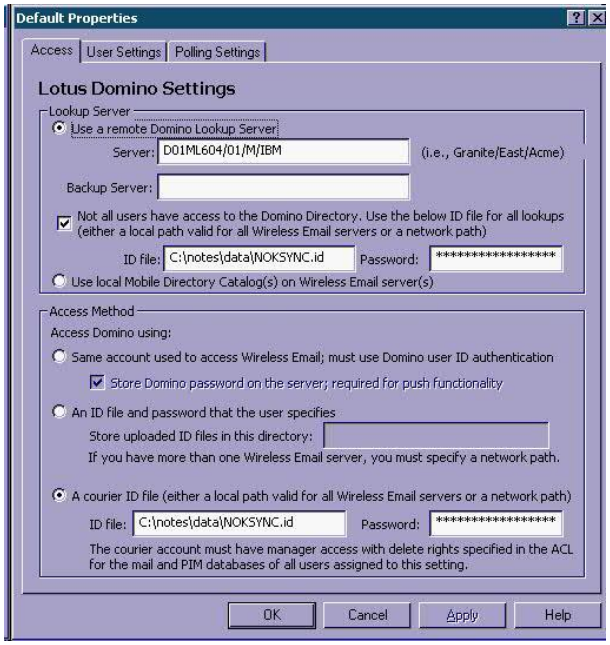

Figure 4. Adding a user with Intellisync

As these examples illustrate, performing even the most basic systems management functions can be problematic and take more time than necessary because of the number of steps to perform each operation, and the need to verify that each step completed normally and without any errors. While not overly complex, these scenarios illustrate the manual intervention required to perform some fairly common actions. The user interface is designed to allow an administrator or technician to perform these tasks as a result of having received a customer service request or a problem ticket.

This type of interaction works well for a one-to-one conversation between a technician and the customer. It requires that at least one technician or administrator be present and have access to the management console. The administrator can perform the required steps to fix the problem and verify the results with the customer. This level of interaction, although beneficial to the customer, is very expensive and doesn't scale.

A typical rollout of mobile phones in a large enterprise may consist of over 5,000 devices, and they are often deployed at the same time in large groups. The ability to provision and deploy a large number of devices at one time was never part of the design of Intellisync. A review of similar offerings from companies such as Sybase,, and seem to indicate that these products were also not designed with a large amount of scalability or the appropriate level of automation to facilitate their use in a large enterprise environment.

C. Enterprise Systems Management Requirements

Managing hundreds or thousands of devices requires a set of tools and technologies that allow the devices to be supported at a low cost while maintaining the appropriate level of integrity and security. In addition to protecting the device from online Trojans, malware or viruses, the management software must insure that the applications and data on the device are safe and secure should the device become lost or stolen, and that the integrity and security of the device and applications is maintained. This requires that the management tools provide the following capabilities.

- Support for Heterogeneous Devices

  Managing a large number of devices in the enterprise requires an infrastructure that supports large groups of heterogeneous devices. Many corporate users have adopted their own mobile device strategy based on their personal needs and preferences.

- Automation of Tasks
- Simplification of Task Directives
- Real-time Monitoring and Reporting
- Policy Directives
- Processes and Workflow

D. Total Cost of Ownership

Over the past decade, much has been made of the cost of ownership for the traditional desktop and laptop computers. Studies have shown that the cost to maintain a PC in the workplace far exceeds the initial hardware investment.

Hardware and software complexities, bug fixes, on-going maintenance, and support desk functions represent the most significant portion of the cost of deploying a personal computer. To control and manage these costs, personal

computers are generally managed through the entire life cycle from initial installation through disposal.

While the management of these desktop systems has proven beneficial, the same model of lifecycle management has not been applied to mobile cellular devices. In most cases, mobile devices go unmanaged through most of their life cycle. Because the devices tend to be small and low-cost, they are not generally viewed as a large investment or ongoing expense.

E. Controlling Device Management Costs

Today's cellular phones are as powerful as some desktop computers and have lots of storage, yet they are not viewed as critical and thus aren't viewed as an important system component that needs to be managed. Their inherent intermittent connectivity complicates monitoring, data protection and software maintenance, even though recent advances in wide-area wireless connectivity have helped mitigate this problem somewhat.

Because they are often switched on and off periodically, the opportunity to perform maintenance on these devices is somewhat limited. This requires the maintenance services to be provided in an intelligent fashion and with knowledge of the device characteristics. Complicating management further is that the number and diversity of these devices precludes manual management other than the management operations initiated by the user.

A recent Gartner study found that 75% of the lifecycle costs of a mobile device came from the management of them. A recent Aberdeen study, *The Real Cost of Enterprise Wireless Mobility*, states:

"It costs nearly 10 times more to manage wireless services and devices compared to wire line. With 80% of respondents planning increases in PDAs with wireless access, these costs are sure to rise. Enterprises in our survey tell us they face two major challenges in supporting wireless mobility: - 64% of survey respondents struggle with escalating costs for services - 57% of respondents rank supporting devices as a close second priority."

Existing offerings in this space, such as Symbol's Mobility Services Platform and Nokia's Intellisync Mobile Suite, have major limitations. They both use piecemeal and propriety approaches, and do not support the end-to-end integration of management processes or the interoperation of tools from different vendors. Further, those offerings are intended as an enterprise solution, and are not appropriate for service provisioning across multiple customers, which impose unique requirements such as customizability, reusability, and global delivery.

III. The Property and Casualty insurance Industry

A. Overview

The property and casualty (P&C) insurance industry is a global, $1,335 billion industry (2005, source: Datamonitor, IBM analysis). This industry protects people and companies from losses stemming from anything from an auto accident to a container ship sinking in a typhoon.

While the financial services industry in general has been the sources of some interesting technological innovations over the years (e.g., the ATM), insurance in particular has not been noted for its embrace of advanced technology. Insurers tend to be very conservative, and their approach to technology generally mirrors that natural conservatism.

Unfortunately for the industry, things have changed significantly in recent years, all of which point to the need for innovation: increased severity and frequency of natural disasters, a growing middle class around the world with more insurable property, a global economy, more stringent regulatory requirements, more competition from both traditional and non-traditional (i.e., insurance-like products from non-insurers) players. And the customers themselves have changed as well. Customers – both individual and corporate – expect a wide range of products offered at low prices. And they expect service to be on demand – by any channel at any time.

Insurance claims processing is one such area of service. It is the area that generates the highest number of complaints – more than 50% according to the National Association of Insurance Commissioners (2005), and some insurers have equipped their adjusters (the people who go out into the field and determine the amount the insurance company should pay on any given claim) with mobility devices such as laptops and mobile phones.

Blue Star will enable insurers to take mobile claims to this next level of service.

B. The Insurance Claims Process

In a typical claims process today, the insured party reports a claim. This often done by phone to a call center, but can be done by Web, by person to an agent or other insurance representative – this is the first notice of loss (FNOL). A customer service representative enters the information and verifies coverage, according to the rules and processes of the insurance company in question.

At some point, depending upon the efficiency of the insurer's processes, a claims specialist (an adjuster) investigates damaged property, re-enters information into the insurer's system, requests and receives appraisals from vendor(s), and negotiates an offer with the insured party. If the offer is accepted the customer (or vendor) receives a payment, typically via a check in the mail.

This is a highly simplified view of the claims process, of course. The underlying processes and the process within each step can be staggeringly complex.

C. Mobile Initiatives in the Insurance Industry

Insurance companies have embraced mobile technologies for claims processing to some extent. Adjusters are often equipped with laptops, mobile phones, blackberries, etc. to make them more effective in their jobs. Progressive Insurance is one example of an insurer using mobile technologies for competitive differentiation: adjusters are dispatched to the scene of an accident ready to write a check. Some insurers also utilize mobile technologies during large-scale claims situations such as hurricanes or other catastrophes. Nationwide Insurance, for example, is one of several U.S. insurers with a mobile claims "command center" – a customized bus equipped with satellite hookups, WLAN connections and other communications paraphernalia intended to speed up the claims process in such situations.

D. Implementing a Mobile Claims Application

The state of the art today for mobile claims processing is the laptop PC. Insurers have customized their claims forms to be saved on their adjusters' laptops, so that information can be captured at the scene. However, to complete the claims process most information and forms are usually stored locally on the computer and later uploaded at the office or mobile command center for review and approval. The resulting delay in claim settlement results in increased overall costs to the insurance company and decreased customer satisfaction. Additionally, this deferred processing paradigm presents a huge enterprise and policy holder security risk should a laptop be lost or stolen. Poor battery life and the availability of secure wireless connectivity have also been particularly problematic during some recent large-scale disasters.

There are a number of drivers for enabling mobile claims in insurance:

- Business Optimization – The claims process and many insurers is high-touch, inefficient, expensive and inflexible. In a very competitive marketplace, insurers are looking for ways to maximize business performance to increase profits and employee productivity while lowering costs.

- Catastrophe Response – P&C insurers with potential exposure to catastrophes need ways to better react during such a crisis. Utilizing mobile solutions to manage activities is one way to drive down the expenses, increase accuracy and speed, and provide a high level of customer service. In catastrophes, an insurer's reputation is on the line as well (e.g., Allstate and State Farm, among others, in the aftermath of Katrina) and a well-managed mobile workforce can mitigate this risk.

- Competitive Advantage – Progressive is one example of an insurer using mobile technologies for competitive differentiation: adjusters are dispatched to the scene of an accident ready to write a check. The opportunity is there for other insurers to do so in many different manners, depending upon their competencies and customer base.

- Demographic Shifts – Experienced, skilled claims adjusters are retiring faster than they are being replaced, requiring better workforce management and capacity planning, and mobility should be central to any redesigned workflow. Not only will that help reduce staff and training requirements for new adjusters, it will also help attract the next generation of highly-skilled workers in the "war for talent" (insurers fighting over a dwindling supply of talented personnel) that many experts see coming.

- Customer Service – As previously mentioned, a majority of complaints about insurers focus on the claims process, in particular delays. Utilizing mobile wireless technologies can be one way of not only reducing the number of complaints, but actually turning the claims process into a point of competitive differentiation.

E. Automating the Mobile Claims Process

Claims adjusting is part art and part science. The best adjusters are the ones with years of experience from which to draw on when investigating a claim. But giving those adjusters – and especially those who are not quite so skilled – the technological tools to help them do their jobs better and faster are a top priority of many innovative insurers.

Mobile claims exist in some part today, for some insurers and in some regions. However, even in a "mobile claims" situation, the process is often not automated. The end goal is to achieve a straight-through process, where the claim is routed to an adjuster based on business rules (with factors such as claim location, type and complexity coming into play), and each step in the process that can be handled automatically, is handled automatically. The human factor only comes into play when absolutely necessary.

F. Standardized Forms and Form Processing

The insurance industry has no one global standard for forms, although there are standards bodies which are trying to promote this goal. Language and requirements will for the foreseeable future depend upon the country, region and/or state in which the insurer operates.

IV. BLUESTAR ARCHITECTURE

This section describes the architecture of Bluestar, and design choices made in an effort to address two of the key pain points faced by the insurance property and casualty industry in adopting wireless technologies for mobile claims processing: 1) the high cost of deploying and supporting large scale wireless, mobile infrastructures, and 2) maintaining existing enterprise security policies in mobile environments.

Bluestar builds upon Autopilot, a framework developed by IBM Research in 2006 for the integration of system management tools. Autopilot permitted automation of system management processes to an unprecedented degree. It was a meta-manager: a manager of system management tools, based on executable process and policy definitions. This system is described in (Mastrianni, 2007).

A. Goals

As previously mentioned, the goals of Bluestar are to provide simplified operation through automation, the ability to integrate with other components and with enterprise applications in order to implement higher-level business processes, and high customizability through policy-driven management.

Automation is implemented with computer-based processes and policies that define the service content. Bluestar provides for automated mobile device provisioning, services deployment and management of large user populations. The underlying software is abstracted through a set of common processes and APIs to provide a uniform view of the management platform. Users need not be knowledgeable of how tasks are accomplished or what tools are being used to implement the systems management tasks.

Bluestar's integration goal is two-fold: internal integration of disparate management tools, and external integration with other components (e.g., service desk) and enterprise applications. These requirements are typical of those addressed by Service Oriented Architectures (SOAs). Customizability is addressed by two kinds of policies: policies concerning device configurations and policies consulted by processes.

B. Challenges

As an integrator and controller of other software components, Bluestar faces several significant challenges: diversity of support for its key function, device management and the tension between reuse and customization.

As mobile devices and their software exhibit great diversity (at the time of writing, there were six major mobile device operating systems) that diversity is reflected in the software that has been written to manage them as well. Examples include Nokia's Intellisync© Mobile Suite and Research in Motion's BlackBerry Enterprise Server. No single suite can manage all mobile devices as well as others can; some devices can be managed by only one suite. Suites differ in their structure, function, management model and command set. Bluestar would ideally be able to work with any suite and with multiple such suites at the same time (to manage multiple device types). Yet it is important for processes and policies to remain free from any suite dependencies.

Reuse is strongly favored by making the Bluestar architecture and various data and definitions independent of any mobile device management suite and of the customer infrastructure, to the extent possible. But, individual customers may have different IT architectures, processes and policies, and these must be respected.

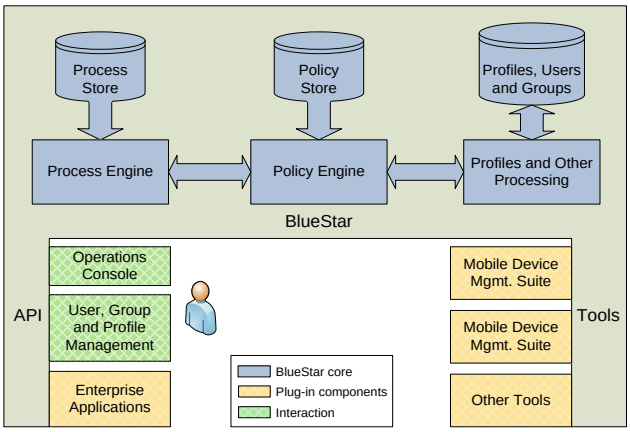

Figure 5. System overview

Figure 5. System overview shows a Bluestar system configuration for mobile system management. Service assets such as policies, processes, profiles, users and groups are shown in blue as symbolic disks. Processes run in a workflow engine, and may contain human tasks. Processes are customized to a specific customer's needs through policies, stored in the policy store and executed in the policy engine. Plug-in software tools are shown below and to the right. Processes choreograph the various management tools in order to implement service definitions. Processes consult policies in order to deliver services customized to the specific needs of a customer. Note that Bluestar manages and controls existing tools to perform system management functions. It does not interact directly with the mobile devices or their software.

C. Service-Oriented Architecture (SOA)

An SOA has been described (Colan, 2004) as a standards-based, loosely coupled, stateless, coarse-grained system, often adhering to the Web Services (WS) standards. **Error! Reference source not found.** depicts an SOA. The messaging infrastructure is an Enterprise Service Bus (Keen, 2004), based on something as simple as direct local Hyper Text Transfer Protocol (HTTP) or as sophisticated as secure messaging and queuing, depending on the packaging of tools and Bluestar services. Due to loose-coupling and no requirements for a common platform for the tools, adding or

substituting a tool is simpler than in tool suites where all tools share a common platform.

The Bluestar SOA is similar to SOAs typically used for enterprise application integration. Its primary goal is the integration of loosely coupled services. Data does flow between services to enable the implementation of complex cross-tool processes. Bluestar also operates under implicit and sometimes explicit time constraints because the processes it automates affect the availability and integrity of the enterprise mobile IT infrastructure. When reacting to a security threat or to a failure, Bluestar must act quickly to contain damage and to restore the mobile IT infrastructure to health.

D. Internal integration

The first challenge to the Bluestar architecture is that it must integrate with its key functional component: the device management suite. To this end, Bluestar defines a Tools interface, as shown on the right in **Error! Reference source not found.** on page **Error! Bookmark not defined.**. This is a Web Service-based interface. Also shown on the left in the figure is the Bluestar API, discussed later in "**Error! Reference source not found.**" on page **Error! Bookmark not defined.**. Integration with the device management suite is also promoted by policy-driven management, discussed on page **Error! Bookmark not defined.**.

E. Policy-driven processes

Mobile systems management tasks in the Bluestar architecture are represented as process definitions, modified by policies, and executed by a workflow engine. This way of representing a task is very flexible, maintainable, and extensible. Process definitions represent the business processes of mobile IT systems management. A process consists of a set of steps that can be performed sequentially or simultaneously. Steps themselves can be processes, and their results can be used in decisions concerning which step is to be performed next. In Bluestar, steps that are not defined as processes are performed by either Web Services (WS) or by purpose-written code fragments.

A process instance represents a systems management task, created by instantiating a process definition. The Bluestar architecture selects a process definition to be instantiated in two ways: either through an interaction with a system administrator using the Bluestar console or programmatically, through process invocation as a step in another workflow. This programmatic selection can be quite involved, as in the case of problem determination, where a process definition is selected on the basis of its being the best remediation of a problem.

Bluestar uses a WS-BPEL-compliant process engine[1], enhanced with human interface features and business rules. Processes can be designed with a process design tool[2] and implemented graphically with a process builder[3].

A typical process would govern software installation, staging the installation files so that they are available to devices, verifying software licenses, making profile changes to require the software on a selected group of devices and logging their successful installation. Such a process would be a component of a higher-level process, provisioning devices according to the role that their users play.

F. Profile-driven Device Management

Profiles are lists of constraints on configuration items like communications, ports, software and settings. For example, a given profile might specify that the USB port on a device be disabled, as a way to prevent the export of data through that port. In Bluestar, profiles are the primary means of device management.

A profile is created for a given device. Each time that device connects its configuration is inspected and if different from its profile, altered to conform. Managing a device is equivalent to managing its profile. Profiles are typically not complete, but govern only those configuration items which must be managed.

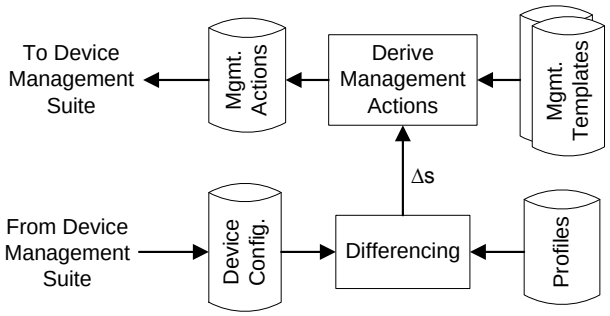

Figure 6. Profile differencing

Figure 6. Profile differencing shows this in more detail. When the device connects its configuration is obtained by the device management suite. That configuration is compared with its profile and deltas obtained, representing non-conformance. Each delta then instances a management template to form a management action which is sent to the device management suite for execution, either at the current time or at a later time when the device next connects.

With some devices it is possible to prevent some or the entire device configuration from being alterable by the end user. For these, an optimization is possible: knowing the device configuration at some past time, and knowing that the user cannot change it, one can infer that any profile change will result in a delta with a corresponding management action. This can be done even before the device connects, so that the management action is waiting for it when it does.

[1] IBM WebSphere® Process Server

[2] IBM WebSphere® Business Modeler

[3] IBM WebSphere® Integration Developer

This style of management has several virtues:

- It is independent of the command set of any specific device management suite.
- In order to change the device configuration it is not necessary to specify how the change is to be done, but rather only the target device configuration.

G. Integration with Enterprise Applications

The worlds of system management and enterprise applications seem to relate to different layers of the software stack. Does it make any sense to link them, as this topic suggests? Here we will try to give some examples of the benefits of exposing management capabilities to enterprise applications, or at least to enterprise business process implementations.

H. Scenarios

Consider the process of bringing a new employee into an enterprise – some call this "on-boarding." Among the effects of on-boarding on IT is the allocation of resources, including capacity expansion as necessary. The resources allocated include end user devices, networking links and ports, addresses, entries in directories and access control lists, software licenses and online storage. Security-related resources include private keys, certificates, capacity related to virtual private networks and security monitoring (e.g., passwords, intrusion). In fact, the impacts of on-boarding on IT can be so extensive as to significantly delay the productivity for which the employee was hired, not to speak of the negative impression on the employee him/herself.

Now, the resource allocation for a new employee is a process of the IT department. These processes differ in detail depending on the enterprise, the division and the role of the employee. An attempt to automate the on-boarding process must include IT.

Today this is done by notifying IT, say in an e-mail, and hoping for the best. But when IT processes can be invoked directly by the on-boarding process, the specifics of the request can be transmitted without error, the specific IT tasks can be identified and the process can be responsive to the results of each step. For example, if a critical employee's on-boarding is being held up by the lack of a software license, this can be expedited.

The danger in linking system management to "higher-level" business processes is added complexity. Some might argue against this linking, as being an inappropriate cross-level subversion of the clean distinction among levels of activity. It is our contention that the business level of high-level IT processes is similar to that of other business processes, and that their linking, as we suggest above, is constructive and indeed necessary to achieve the rapid, accurate response by the organization to changing business needs.

I. The Bluestar API

The Bluestar API has three components, of successively increasing specificity. These are *process invocation*, *profile management* and *data access.*

An enterprise application can interact with Bluestar by invoking one of its processes (processes are discussed in "**Error! Reference source not found.**" on page **Error! Bookmark not defined.**).

Appropriate input should also be provided, in accordance with the process definition. Process status can be monitored, and process results obtained. Process invocation and process interaction both benefit from process standards.

An enterprise application can interact with Bluestar by changing profiles (profiles are discussed in "**Error! Reference source not found.**" on page **Error! Bookmark not defined.**). When a profile is changed all of the devices governed by that profile are subject to configuration change in order to conform to the new profile.

This direct interaction between an enterprise application and a device configuration should not be routine; most such interactions should result from the application invoking a process whose effect is to change the profile. In this way, policy can be more easily observed, and the specifics of device management can be hidden.

An enterprise application can interact with Bluestar through data access; say to retrieve specific information from a log or to examine statistics on connection performance.

Applications can change the group structure and membership, create new profiles and associate them with groups, manage policies and delete users. These actions should probably not be performed directly by an application unless it is written for the specific purpose of reorganization, but rather should be performed by invoking a process which performs the desired functions. Again, this supports policy enforcement and information-hiding.

V. Transforming Property and Casualty Claims Processing with Bluestar

A. Transforming the Enterprise

In the past few decades, IT engineers and scientists have been using information and communication technology to reshape economic and social activity across all sectors. Business process is a critical element in enterprise transformation. Enterprises require processes in the form of end-to-end solutions in order to effectively link internal and external business applications, systems, and staff. These solutions enable them to respond with flexibility and speed to complex and changing business conditions. Transforming the

insurance property and casualty claims processing industry to fully leverage the benefits of wireless mobility is one such example. This transformation can add value to customers and lead to higher productivity and lower operating costs.

B. Bluestar Support for Insurance Claim Processing Scenarios

To illustrate how Bluestar can help facilitate the transformation of a claims process to a highly-scalable, automated and secure mobile environment, we introduce three typical scenarios centered on the wireless mobile management, scalability and security aspects of property and casualty claims processing. The first scenario represents the idea of profile-driven process automation in mobile service management. The second one shows the integration of a mobile platform with enterprise IT applications. The third shows the utilization of a standard interface for device management tasks.

In the first scenario, an insurance company purchases a number of smart phones for their property and casualty claims adjusting department. To configure these mobile devices for remote processing, the smart phones must have the necessary claims processing application and policy information installed. Bluestar provides an integrated management interface for administrators to facilitate configuration of all the mobile phones for the claims application. First, an administrator of the Bluestar server selects the appropriate property claims application. Next, using the device management features of the mobile device management suite, Bluestar automatically queries each mobile phone via the wireless network, determining each device's unique characteristics and capabilities, matching it against a profile of operational requirements of the claims application. Bluestar and the device management suite then perform all necessary firmware, driver or application updates, making the mobile phone ready for use by the claims adjuster.

In the second scenario, an insurance company's customer service center has received a first notice of loss call from a policy holder. To automate the identification and assignment of an adjuster to settle the claim request, Bluestar assists the administrator by locating the closest available adjuster utilizing the GPS location data acquired through the mobile device management suite, and correlating this to a corporate, shared calendaring and scheduling facility. Bluestar then helps to assign the claim request to a specific adjuster, update the calendar and scheduling database, push necessary policy holder information, location and nature of the damaged property, and information gathering forms to the adjuster's mobile phone, and upload detailed damage photos to the home office for review and approval of payment (see Figure 7. Claim submission).

Figure 7. Claim submission

In the third scenario, an insurance company administrator receives notice that an adjuster's mobile phone containing company and individual policy holder data has been lost or stolen. The administrator locates the adjuster's profile and mobile phone record, then sends a "Device Lock and Wipe" command to the mobile phone, erasing calendar, contact, email and other corporate or policy holder information, and blocking the device from performing from any other operation, including re-boot.

VI. PROTOTYPE AND PILOT EXPERIENCE

A. Bluestar Pilot

Bluestar provides a generalized device management infrastructure that can be applied to any type of mobile industry, deployment, or application. The first deployment of Bluestar targets a mobile claims application for the Property and Casualty insurance industry.

However, Bluestar can also be used to manage a base set of applications which we believe to be necessary for any type of deployment. These applications include e-mail, calendar, address book, and to-do lists, and represent the minimum complement of applications that should be installed on a mobile device to make that device acceptable as a platform for enterprise mobile applications. At a minimum, Bluestar must be able to leverage the key features of simplification and automation in the management of these applications.

To validate the management features of Bluestar, we instituted a pilot program using a prototype configuration of the Bluestar software utilizing Nokia's Intellisync Management Suite for device communications and provisioning, Bluestar's process-driven management to provide the simplification and automation required for enterprise deployment, and Lotus Notes Domino.

Access to the management suite is enabled through an administrator login on the intranet web site, and also enabled

from the Internet through the Nokia Secure Gateway component of Intellisync. The Secure Gateway provides a point of contact from the Internet in the yellow zone. It provides one-way outgoing communications from the Intellisync server to the gateway, but no incoming connections from the gateway. This provides an adequate level of security to isolate the corporate intranet from the mobile devices on the Internet. User access to the web site is enabled through a normal Internet URL (see Figure 8. Intellisync Mobile Suite User Access).

Figure 8. Intellisync Mobile Suite User Access

Twenty users were given a variety of mobile phones manufactured by Nokia, Samsung, Sony, Motorola, and Palm. These phones run a variety of operating systems including Symbian S60, Palm, and Windows Mobile. The pilot users had little or no prior experience with these devices, and were supplied the phones direct from the manufacturer without any special software installed. Users were supplied a telephone number and instructed to connect to their specified wireless carrier and then contact the Bluestar web site to receive further instructions.

B. Pilot considerations

The deployment of a pilot program such as Bluestar is subject to intense scrutiny because of the potential security risks any time an external system is allowed access to a system inside the corporate firewall. One solution involves using a mechanism such as the Secure Gateway to isolate traffic from the Internet, while another common solution is to establish a VPN connection from the client into a VPN gateway.

Establishing a VPN connection, however, requires a VPN client on the mobile device that communicates with a corresponding server in the enterprise. Many mobile phones do not have a VPN client installed as part of the standard software shipped on the device and therefore requires that a VPN client be installed on the mobile device. Because each device type runs a different operating system, a VPN client must be supplied for each platform. This also requires the client device to perform the decryption which tends to be compute-intensive.

For the purposes of the Bluestar pilot, we elected to use the Secure Gateway architecture to control access to internal network resources. To utilize the 'push' features of Intellisync, the firewall must be configured to open a port to be used for the push operation. This adds a potential security risk but the risk can be mediated with the proper firewall configuration utilizing stateful packet inspection techniques.

Malware, viruses, Trojans, and key loggers are a concern for mobile devices as well as desktop systems and servers. Although we've not seen any large-scale attacks yet, we are confident that hackers will turn their attention to wireless mobile devices as a new target of opportunity. It is imperative that mobile devices be supplied with the appropriate ant-virus and antispyware, and that they be kept up-to-date with the latest software patches and security updates.

We expect that as mobile devices become more sophisticated and their usage increases that the in their capabilities and become more pervasive that the malware attacks will increase accordingly. To minimize the impact of these attacks, it is important that the management system provides the latest patches and security updates, and enforces them through policy directives. The management system should take proactive actions to insure the security and stability of not only the client devices, but the security of the internal network as well.

C. Pilot goals

The Bluestar pilot provides a proof-of-concept that is deployed to a small group of users. The pilot program provides e-mail, calendar, and messaging, and provides limited access to internal network resources such as databases and files. The pilot project brings together the tools and technologies that can later be packed to provide an integrated solution. A substantial benefit of the pilot project is that the pilot customers get to use the technology as their primary source of information, and the feedback is passed directly to the developers without going through a multi-level support organization. Developers get to hear first-hand the type of problems faced by the users.

The pilot program is deployed and administered through IBM's Technology Adoption Program (TAP). The TAP program is used internally in IBM to bootstrap new technologies and to give employees a chance to use and rate the technologies before they are considered as a customer offering. Participants are generally early adopters who are not afraid of trying something novel or new, and not afraid to pick up the phone when they have a problem or question. The result is that developers receive early valuable feedback on the usability, reliability, and effectiveness of the technology. This feedback is critical to the success of a prototype, and determines whether or not the prototype will be considered as a product or service offering.

Project forums are also available to provide a community where users can openly discuss their experiences and offer workarounds to problems they've encountered. The information and discussions provided by the forum gives developers a valuable resource to help them improve the product. If the technology doesn't work satisfactorily for IBM's internal users it will be reviewed to determine if the project should be reengineered or abandoned.

Since IBM's internal customers are Lotus Notes users, the Bluestar pilot provided support for Lotus Notes e-mail, calendar, to-do, and address book[4]. The pilot initially leveraged Lotus Notes 7 but had now been upgraded to support Lotus Notes 8. Pilot customers are urged to use their mobile phone exclusively for their email and PIM functions.

User demographics including IDs, passwords, entitlement, and authentication information was gathered from a standard LDAP directory. This feature provides a mechanism to quickly configure and provision a solution based on an existing infrastructure. This greatly decreases the time and complexity normally required to provision a program such as Bluestar.

The ability to quickly provision and deploy a secure mobile solution is critical for use in a catastrophic situation such as a hurricane or flood where response time is important.

CONCLUSIONS AND FUTURE RESEARCH

The early deployment of wireless devices exposed several problems related to the management of mobile devices in a large enterprise, and helped define the goals and architecture of Bluestar. One of the most important features that helped shape the design of Bluestar is the ability to perform device and applications management in an automated fashion, and on a large scale. Managing user accounts, entitlement, and access permissions for a few users is not difficult, but providing the same level of support for dozens or hundreds of users is impossible without the proper level of automation and support for policy directives.

Without Bluestar, the relatively simple process of adding a user often turned out to be problematic because of inconsistencies in user IDs, passwords, and even simple spelling errors. When as problem occurred, a human would be required to get involved and interact with the customer through a phone call, and the technician would have to fix the problem by reading log files to ascertain what the cause of the failure was. Once the cause of the problem was found, the technician would then have to log on to the Intellisync server and make changes, stop and restart the Intellisync server, and then verify that the problem was fixed, often with the user still on the phone.

[4] Although we view instant messaging as an important component of enterprise mobility, this feature was not deployed as part of the pilot.

Our investigation into similar management tools revealed that the same type of manual interaction is required to perform many common day-to-day systems management functions. This model of interaction does not scale in an enterprise and requires a relatively expensive support infrastructure including people, equipment, and training. The main focus of Bluestar is to minimize the amount and form of day-to-day interaction required to support a large number of enterprise users. Bluestar's automation and process-driven policies dictate and proactively enforce corporate mandates, insuring that the security and stability of the corporate network is maintained with a minimal amount of human intervention.

Without Bluestar's systems management capabilities, system and event monitoring was performed by manually scraping multiple log files. Often the events captured in the logs have insufficient descriptions to easily diagnose to root cause. In a clustered server environment monitoring the systems must be done individually on each server instance. This approach would obviously not scale in a large enterprise installation. Tools for predictive analysis, modeling scenarios, or monitoring system events for tends, are not provided. In fact there are no capabilities to predetermine potential resource/user issues and act appropriately.

A. Work on our BlueStar pilot for the property & casualty claims industry is not complete at the time of the writing of this paper, and hence our presumptions as to the impact of its process and policy management on the ability to automate and enable the scale out of very large scale secure wireless mobile enterprise deployments cannot not yet be fully validated. There are significant interim results, and several important conclusions we can draw from the work done so far:

1) Software tools for deployment and device management of wireless mobile devices are available, but when used "as-is", cannot provide cost effective, highly scalable wireless mobile environments for enterprise application, such as property and casualty claims processing. Limited results on the scalability of our internal enterprise email pilot, which is a key element of our property and casualty pilot, have validated the need for an automation and management facility such as BlueStar, and demonstrated measurable saving in time and labor costs.

(Is there any rough quantification of this in anything Drew has sent us that we can quote ? or can we get him to estimate what automation might save him???)

2) Available wireless device management software tools have some provisions for basic mobile device security, such as passwords, but almost nothing for managing or controlling proprietary data on the mobile devices.

3) …..

APPENDIX

Appendixes, if needed, appear before the acknowledgment.

ACKNOWLEDGMENTS (GO HERE)

REFERENCES

[1] Colan, M. (2004, April). Service-Oriented Architecture expands the vision of Web services. *IBM DeveloperWorks.*.

[2] Keen, M. et. al. (2004). *Patterns: Implementing an SOA Using an Enterprise Service Bus.* IBM Redbook SG24-6346.

[3] Mastrianni, S. et. al. (2007). IT Autopilot: a flexible IT service management and delivery platform for small and medium businesses. *IBM Systems Journal , 46* (3).

AUTHOR LIST

Steve Mastrianni *IBM Research Division, Thomas J. Watson Research Center, P.O. Box 218, Yorktown Heights, New York 10598 (stevemas@us.ibm.com)*. Dr. Mastrianni is a senior software engineer currently writing autonomic and services software. He holds a B.S. degree in business administration and M.S. and Ph.D. degrees in computer science. He joined IBM Research after running a software development and consulting company for a number of years where he specialized in operating systems development, device drivers, real-time applications, data acquisition, and 3D graphics. Dr. Mastrianni is the author of three programming books, numerous conference papers, and has written over 100 articles for industry trade publications. He has 24 issued patents.

David F. Bantz *IBM Research Division, Thomas J. Watson Research Center, 19 Skyline Drive, Hawthorne, New York 10532 (dfbantz@us.ibm.com)*. Dr. Bantz was a research staff member from 1972 to 2005 after a short stint with a startup. He graduated from Columbia University School of Engineering and Applied Science in 1970 with an Eng.Sc.D. degree and taught there and at the University of Southern Maine as an adjunct professor for over 30 years. He has 29 issued patents. His technical interests have always been in personal computing applications and technology, and he is currently working on automated systems management.

Tom Chefalas *IBM Research Division, Thomas J. Watson Research Center, P.O. Box 218, Yorktown Heights, New York 10598 (chefalas@us.ibm.com)*. Mr. Chefalas is a Senior Technical Staff Member in services technologies. He received a B.S. degree in computer science in 1988 and a M.S. degree in computer science in 1992 from New York University. He joined IBM in 1987. Mr. Chefalas is currently working on desktop management, autonomic computing, and end-user services.

Song Jinho, *LG CNS Co., Ltd. (jsong@lgcns.com)* TI specialist and Technical Research Engineer 부책임연구원, LG CNSCo., Ltd, Trutec Bld. 4th Flr., Digital Media City B6-2, Sang-ahm-dong, Ma-po-gu, Seoul 121-270, Republic of Korea.

Dong Jun Lan *IBM Research Division, China Research Laboratory, Building 19, Zhongguancun Software Park, 8 Dongbeiwang West Road, Haidan District., Beijing 100094, People's Republic of China (landj@cn.ibm.com)*. Mr. Lan is a researcher in the High Performance Solution team at the IBM China Research Laboratory. He received his M.S. degree in electrical engineering from Tsinghua University, Beijing, China. Mr. Lan has published more than ten papers in international conferences and holds five patents.

Gary Leonardi, *IBM Research Division, Thomas J. Watson Research Center, P.O. Box 218, Yorktown Heights, New York 10598 (leonardi@us.ibm.com).* Mr. Leonardi is a Senior Network Engineer with 18 years of experience in the fields of information technology and services. His current responsibilities include the development and deployment of advanced wireless and remote access solutions for IBM. His current focus is wireless security and remote access.

Pei Ni Liu *IBM Research Division, China Research Laboratory, Building 19, Zhongguancun Software Park, 8 Dongbeiwang West Road, Haidan District., Beijing 100193, People's Republic of China (liupeini@cn.ibm.com). Ms. Liu is a research & development engineer in the IT Service Management team at the IBM China Research Laboratory. She received her M.S. degree in systems engineering in 2005 from Xi'an Jiaotong University, Xi'an, China. Her current focus is IT service management and device management.*

Randy Moulic, *IBM Research Division, Thomas J. Watson Research Center, 19 Skyline Drive, Hawthorne, New York 10532 (rmoulic@us.ibm.com).* . Dr. Moulic is an IEEE Fellow and Research Staff Member at the IBM Thomas J. Watson Research Center. He participated in the development of many high performance and personal computing systems, including the RS/6000/Scalable Parallel supercomputers, IntelliStation, and Cell/B.E. processor graphics workstations, ThinkPad ''TransNote'' laptop, and QS20 Cell/B.E. processor server. He founded, organized, and directed the Deep Blue computer chess project, initiating the first exhibition match events with World Champions Gary Kasparov and Anotoly Karpov. He has authored many technical papers, holds many patents, and is an Adjunct Professor at Columbia and Polytechnic Universities.

Dennis G. Shea *IBM Research Division, Thomas J. Watson Research Center, 19 Skyline Drive, Hawthorne, New York 10532 (dgshea@us.ibm.com)*. Dr. Shea is a Senior Manager in the Services Research department. He holds B.E. and M.E. degrees in electrical engineering from Rensselaer Polytechnic Institute, an M.A.S. degree from Florida Atlantic University, and a Ph.D. in computer science from the University of Pennsylvania. He began his career at IBM Boca Raton working on small systems and his technical interests have revolved around connectivity, mobile solutions, and client management services. Dr. Shea's current interest is in the area of service sciences research and its application to solving customer problems.

JiSeong Song, *LG CNS Co., Ltd. (jissong@lgcns.com)* TI Senior Leader 총괄연구원, LG CNSCo., Ltd, Trutec Bld. 4th Flr., Digital Media City B6-2, Sang-ahm-dong, Ma-po-gu, Seoul 121-270, Republic of Korea.

Drew Wyskida, *IBM Research Division, Thomas J. Watson Research Center, P.O. Box 218, Yorktown Heights, New York 10598 (wysk@us.ibm.com.)*Mr. Wiskida is a Senior Network Engineer with 18 years of experience in the fields of information technology and services. His current responsibilities include the development and deployment of advanced wireless and remote access solutions for IBM. His current focus is wireless security and remote access.