



Building the Wireless Enterprise:

The Isovia M-Business Platform

White Paper

All rights reserved. Isovia, Inc. © 2000

111 Devonshire Street, 3rd Floor • Boston, MA 02109

Table of Contents

White Paper	1
Introduction.....	3
Audience	3
The Challenge of Enterprise Systems	Not Included 4
Isovia M-Business Platform.....	7
Direct Access to Enterprise Applications	Not Included 7
Multiple Enterprise Systems.....	Not Included 8
Building Mobile Applications.....	Not Included 8
Many Mobile Devices.....	Not Included 10
Security Features.....	11
Alerts and Notifications	12
Working Offline.....	Not Included 14
Voice	Not Included 15
Monitoring and Administration	Not Included 16
ASP or Product.....	Not Included 19
Implementation Technologies.....	Not Included 20
100% Pure Java	20
Scalability.....	20

Introduction

The Isovia M-Business Platform enables large enterprises to realize the benefit of delivering information when and where it is needed. The industries that profit from this solution are numerous – virtually any large company can save time, effort, and money if it can provide timely information on the spot to its mobile workers.

There is no shortage of concrete examples where measurable ROI exists for the deployment of an **enterprise grade** wireless solution. (Note: *enterprise grade* refers to the effective handling of network latency, limited bandwidth, spotty network coverage, and device memory constraints when deploying mission critical enterprise applications). Examples throughout this document cite many of the operational improvements experienced by Isovia's customers within sales force automation, customer relationship management, and field force automation.

The applications and benefits are only possible if the solution implemented is **enterprise grade**. The Isovia M-Business Platform was designed and built by world-class engineers to provide a solution that CIO's can endorse as capable of delivering true ROI. This white paper discusses the components of the Isovia M-Business Platform and the requirements that led to its design and architecture.

Audience

- CIO's
- Technology strategists and senior managers.
- Software engineers and other developers using the Isovia M-Business Platform.
- Network architects and engineers.
- System administrators and other IT professionals.

Isovia M-Business Platform

The **Isovia M-Business Platform** is specially designed to enable access to Enterprise applications and data. Mobile enterprise applications have unique requirements that cannot easily be met by retrofitting existing enterprise systems, or by modifying mobile systems that were originally designed for B2C (Business to Consumer) applications. Figure 1 provides a high-level illustration of the **IMP** and the next few sections describe the different components of the overall solution.

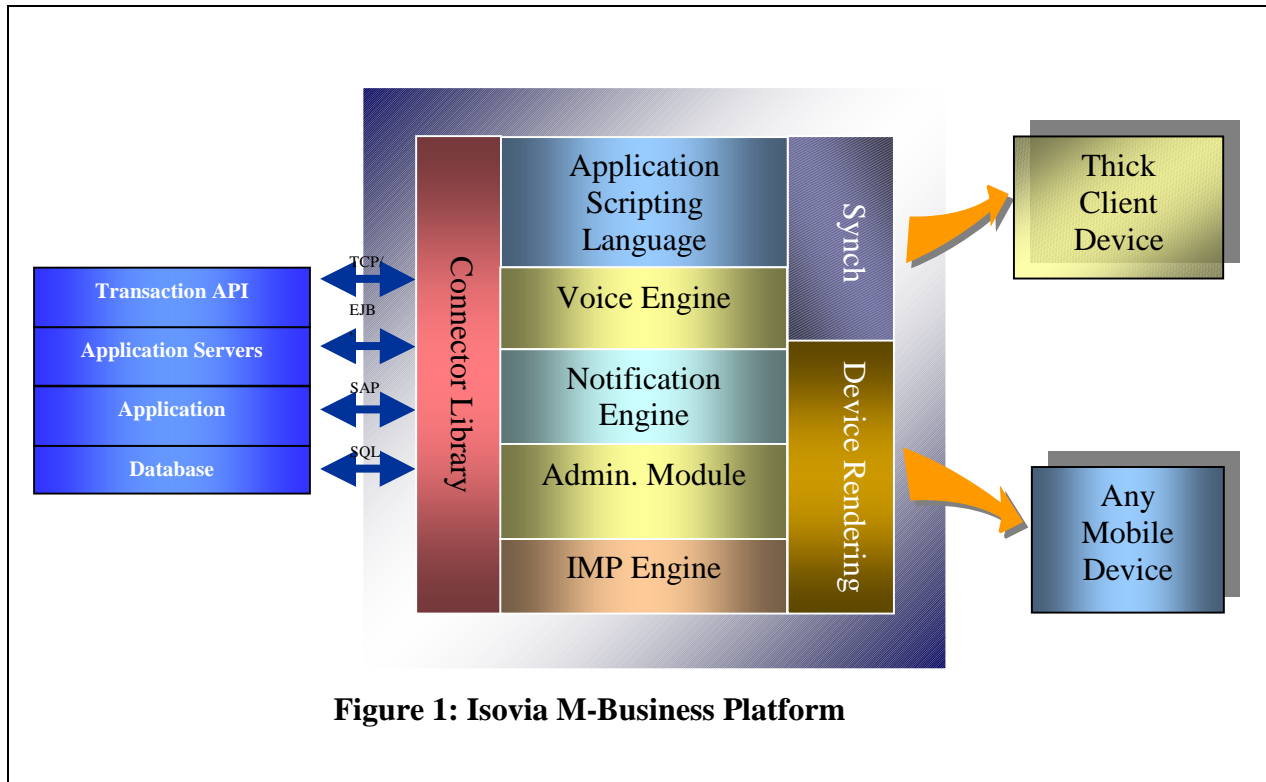


Figure 1: Isovia M-Business Platform

Isovia M-Business Platform

Sections Not Included:

Direct Access to Enterprise Applications

Multiple Enterprise Systems

Building Mobile Applications

Many Mobile Devices

Working Offline

Voice

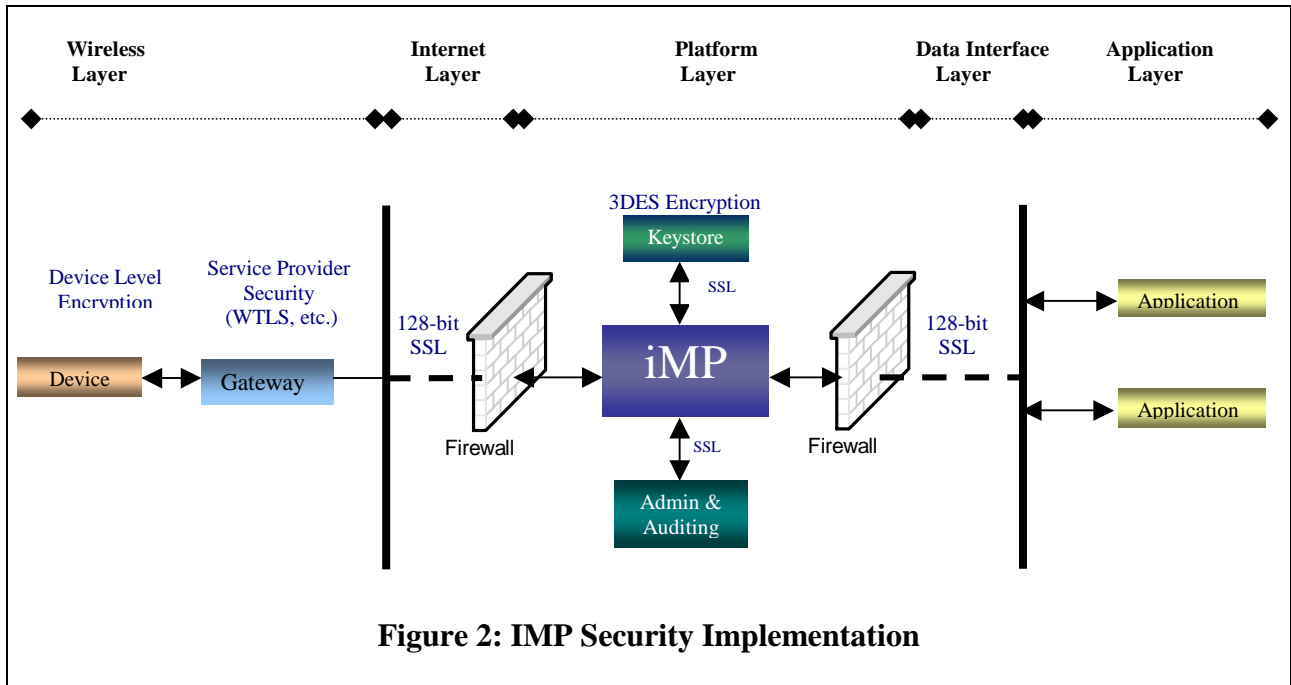
Monitoring and Administration

Security Features

Requirement #5:

Mobile applications must not compromise the security of Enterprise data.

There is no single answer to maintaining security. Security must be integral to the platform and to all communications across the platform, right down to the security of the data in the mobile devices.



Security in communication: **IMP** uses industry security standards, such as SSL to encrypt both platform to device communication and platform to Enterprise back-end communication. Data is protected within the **IMP** platform because:

- The **IMP** platform does not persist user credentials¹, or perform user authentication. User authentication is performed against a backend Enterprise system.
- **IMP** does not store user data across sessions.
- Session data is encrypted within **IMP** between interactions².
- Anti-spoofing measures in **IMP** prevent session hijacking².

In other words, **IMP** only deals with Enterprise data as it passes through the platform. By not storing Enterprise data, the risk of exposing sensitive information is minimized. To further protect data, the **IMP** platform can be deployed behind a firewall, as it is in Isoviva's own ASP practice (and as we would expect in any corporate deployment). Figure 2 describes the end-to-end implementation of security in the **IMP**.

¹ However, the Alert and Notification feature might store user contact information, the authentication of which should come from the back-end system.

² This is a planned feature for release 2.9.

Alerts and Notifications

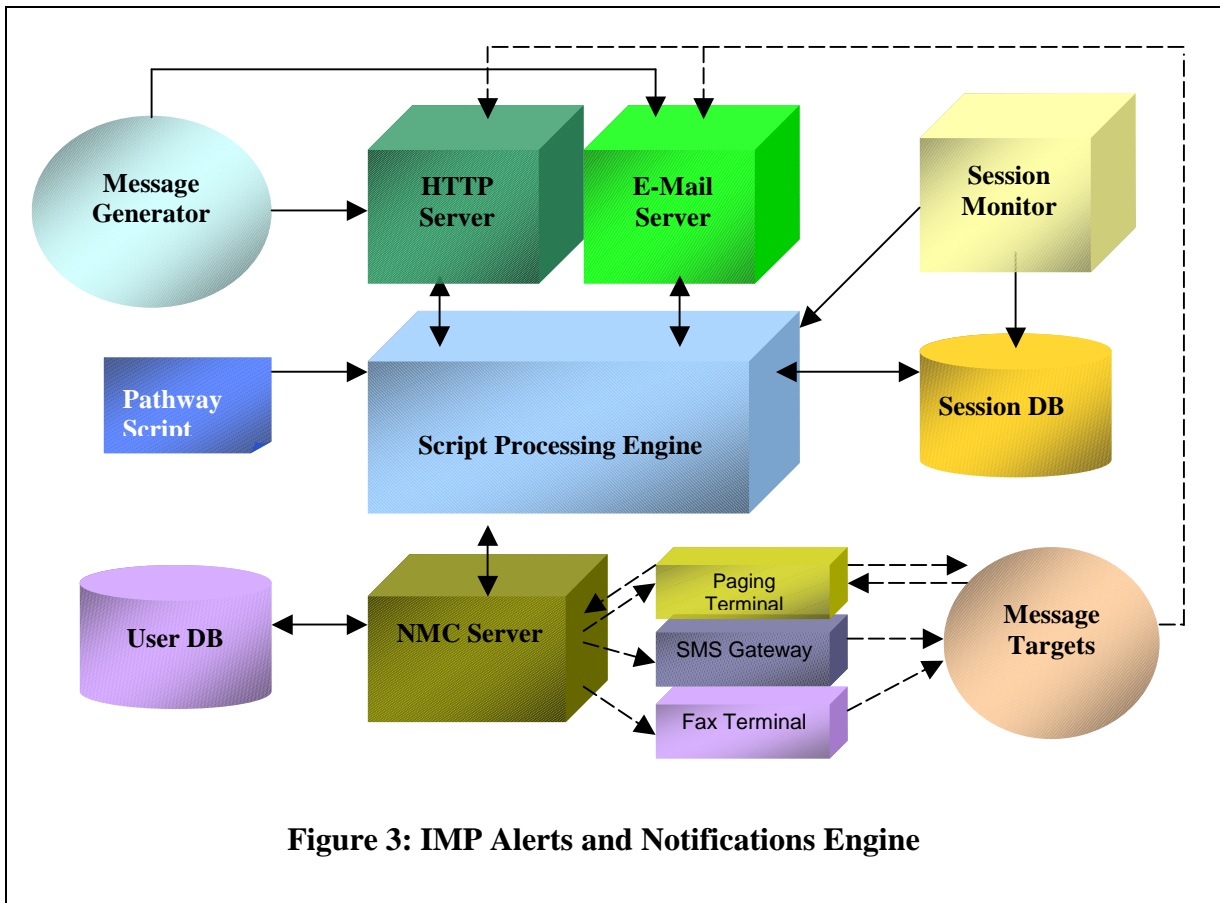
Mobility implies being able to work any time, anywhere. Requirement #6:

A mobile platform should provide the ability to send alerts or notifications anytime, anywhere.

iMP provides an industrial strength notification and alert facility as shown in Figure 3.

- Alerts can be sent to a variety of devices – pagers, cell phones, e-mail, faxes, etc. The multi-modal capabilities of **iMP** mean that an alert does not need to use the same device that the user may have used to start the transaction. In other words, a salesman might submit an order via a Palm Pilot, but an alert concerning the order (e.g. “customer exceeded credit limit”) could be sent via a pager or SMS message.
- Alerts can receive and require responses. In the case of a pager, the response could take place in real-time and delivered back via the same device as the alert. However, for other devices the response might use a different mode. For example, a faxed alert might contain the URL of a page where a response should be entered.
- Alerts can cascade. In other words, if the desired response is not received within a certain time period, an alternative action can be taken (e.g. alerting the next person on the list).
- Alerts can be broadcast. More than one person (or entity) can be alerted at the same time.

The multiple device and cascading nature of the alerts are performed via an **ASL** script, and can thus implement any policy that is appropriate for the **business process** of the application.



Facilities are provided for registering and maintaining contact information needed for alerts (e.g., pager numbers, cell phone numbers, email address, etc). This can done via the **IMP Management Console** or, to alleviate the burden on administrators, applications can be set up to allow users to self-register. For example, the first time a salesperson uses the system he can be directed to a screen that lets him enter his cell phone and pager numbers.

Chapters Not Included:

The Challenge of Enterprise Systems

ASP or Product

Implementation Technologies