Powering the Bank in Your Hand

White Paper

BlueIce Research

infovention

COMPAQ

intel

Table of Contents

Blueice™ Research*

Founded in February 2000, Blueice* Research* develops security solutions for all types of situations demanding digital identification, signatures and receipts. The financial sector is currently the primary target for these solutions. Blueice Research's flagship product, the Multipass*, allows users of mobile phones and handheld computers to conduct secure transactions on the mobile Internet with great ease. The Multipass is used to confirm the identity of the user and to create digital signatures that cannot be later repudiated by any of the involved parties. The Multipass runs on the most common operating systems that are used on handheld computers today, namely the Palm OS*, Pocket PC*, EPOC* andWin32*. Blueice Research's partners include Nexus*, Entra*, TAJT* and Infovention*.

www.blueiceresearch.com

infovention

Infovention is an IT consulting company whose mission is to deliver a full range of high quality business solutions to the finance service sector Infovention's strength lies in our balanced expertise, which includes project management, commercial insight based on
experience of different sectors, in-depth technical and strategic expertise and a quality-assured approach to our work. Together, these ensure that we can supply high-quality turnkey projects on a fixed-fee basis. Having worked with some of the Nordic region's largest banks on mobile banking strategy projects and mobile banking solutions, Infovention has gathered extensive experience from the field. Infovention acts as an independent consultant and assesses new products and platforms for mobile solutions. This work is ongoing in order to ensure that we can offer clients the solution that best suits them and their current situation. Based on our expertise we have developed a Mobile Banking Component library, from which Bank-in-your-hand has been developed.

www.infovention.com

Intel

As a leader in Internet and business technologies, Intel is committed to enabling the evolution of e-Business. At Intel, a new e-Business service generated more than $1 billion in its first month. Its vision is a horizontally integrated environment, where the solution comes from many different vendors. Horizontal integration involves selecting best-of-breed hardware and software from a wide range of vendors and mixing and matching it to meet individual needs.

The benefits of this approach, which is pioneered by the Intel® Architecture, are faster innovation, a wider choice of operating systems and application software packages, and better cost-effectiveness derived from increased competition. Intel aims to deliver the essential tools for dealing with the uncertainties of today's e-Business environment. It is a premier supplier of building blocks for the Internet economy providing clients, servers, networks and services.

Intel also works with hardware vendors, independent software vendors, operating system vendors, solution providers and end customers. Its aim is to enable an open e-Business environment and to accelerate the development of products and services so that vendors and customers alike have flexibility, adaptability, and freedom of choice.

www.intel.com

Compaq

Compaq is a key player in the infrastructure of the finance industry. The top fifteen exchanges, over 90% of the world's securities transactions, the majority of the world's payment systems and ATM networks are served and supported on Compaq technologies. Compaq is investing both internally and with its partners to offer financial enterprises a secure and cost effective route to building new technology-based services and businesses.

Compaq Computer Corporation, a Fortune Global 100 company, is a leading global provider of technology and solutions. Compaq designs, develops, manufactures, and markets hardware, software, solutions, and services, including industry-leading enterprise computing solutions, fault-tolerant business-critical solutions, and communications products, commercial desktop and portable products, and consumer PCs that are sold in more than 200 countries. Information on Compaq and its products and services is available at

www.compaq.com

Summary

The use of wireless communications is now gathering pace. Leaving behind early experimental applications, mobile commerce and mobile finance are now moving towards mainstream consumer use. Faster wireless networks, improvements to handset designs and new business models for mobile applications are all being developed worldwide.

M-Finance and m-Commerce enable banks and retailers to add new delivery channels to their existing services. They can also use the unique capabilities of mobile devices and wireless networks to create innovative ways of interacting with customers. These could include mobile portals which bring the benefits of joint partnerships between organisations to customers, and new payment methods.

However, in order to make these exciting plans become reality, traditional problems of bandwidth availability, security and manageability also have to be considered. As 3G-style networks move towards offering permanent connections to public wireless networks, the risks of data theft and other forms of disturbance such as viruses will also increase.

To make the most of applications such as streaming media, which have been proposed for wireless networks, mobile handsets will need significant processing power. In order to reduce bandwidth congestion, streamed data can be sent in a small, compressed format, which is then processed by the handset itself. Although this reduces demands on the wireless network, it means that handsets will need to be designed in a radically different way from those in use today.

To address these challenges associated with rapidly developing new wireless handsets and handhelds, Intel introduced Intel® Personal Internet Client Architecture (Intel® PCA). The Open architectural framework of Intel® PCA has been designed to streamline hardware development and stimulate software development by providing:

- A Scaleable Architecture maximizing the ability to reuse applications across many segments
- A Parallel development environment for Computing subsystem and Communication Subsystem thus accelerating product time to market
- Applications to be written to high performance and low-power general-purpose processors
- A Flexible and Adaptive Architecture to facilitate integrating new hardware and software features as industry standards and market needs evolve.

Blueice Research's* Multipass* Client* and Server* technology address the equally important area of wireless security. The products provide an end-to-end security solution that is easy to operate, both for businesses and for their consumers. Compatibility with a wide range of mobile device operating systems is a significant benefit of the Multipass Client. It also offers a browser based security system, making it simple to implement. The Client encrypts data offline, ensuring that if a device is lost, the data remains safe. In its online mode, it provides a means of transferring data to a Server application securely.

The Multipass Server offers equally robust security features, and can be scaled across multiple web servers. This means that even the most successful m-Business can ensure its customers remain secure.

Given the importance of both security and ease of use in the finance industry, the result of the first collaboration between Intel and Blueice Research, the *Bank-in-your-Hand*, offers a powerful solution. Developed in conjunction with Compaq* and Infovention*, who provided hardware support and banking applications respectively, this innovative approach to m-Banking provides a new platform that will enable banks to fully explore the potential offered by mobile finance.

Business Background

Mobile Communications and the Consumer Market

The emergence of wireless communications offers a new consumer channel for many types of business. In particular, financial institutions have begun to experiment with the potential of m-Finance, and consumer services are adding value to their services, both through the use of m-Commerce and other value-added techniques.

Although this comparatively new business method is still evolving, improvements in wireless network capabilities and better handset designs are broadening the potential for this market. Many consumers already have a mobile phone or PDA (Personal Digital Assistant) device, meaning that the ideas behind remote working are already well established. However, technology and communications capabilities are only now beginning to catch up with consumer requirements.

Business benefits

The business reasons for banks and other financial services providers to establish a presence in the wireless area is not just to profit from the addition of a new retail channel. They can also use its potential to offer new types of service, or to extend the capabilities of present offerings. These could include joint initiatives with other service providers, such as collaborations between banks and telecom providers.

This pattern of innovation and collaboration reflects trends in the more established e-Commerce and e-Banking markets, as seen in Figure 1. This shows e-Banking moving beyond traditional transaction-based services towards value-added initiatives such as account aggregation, a concept that draws together a customer's financial data from multiple institutions and displays it on a single web page, enabling the customer to see an overview of this data for better financial planning.

A service such as account aggregation would not have been possible using any current banking channel other than the Internet. In the same way, services that are unique to m-Finance will emerge over time.

The Current Wireless Market

Identifying suitable applications for mobile working has been a challenge for both services providers and telecommunications companies. Both the corporate and consumer markets have provided opportunities for developing new applications, but both have been limited by the current status of the technology itself.

Mobile devices at work

Business-to-Employee (B2E) mobile device use is one of the fastest growing areas of wireless communications. The challenges involved in offering mobile services within the workplace are different from those associated with consumer use. Issues such as scalability, security and availability offer less daunting challenges in the business environment. For example, it's possible for organisations to clearly identify the number of users and the types of device that will be connecting to a service, and to specify rules for how an application must be used. Handheld devices, such as Palm* and Microsoft* Windows* CE machines like the Compaq* iPAQ* and Pocket PC devices have also penetrated business environments more successfully than consumer markets so far.

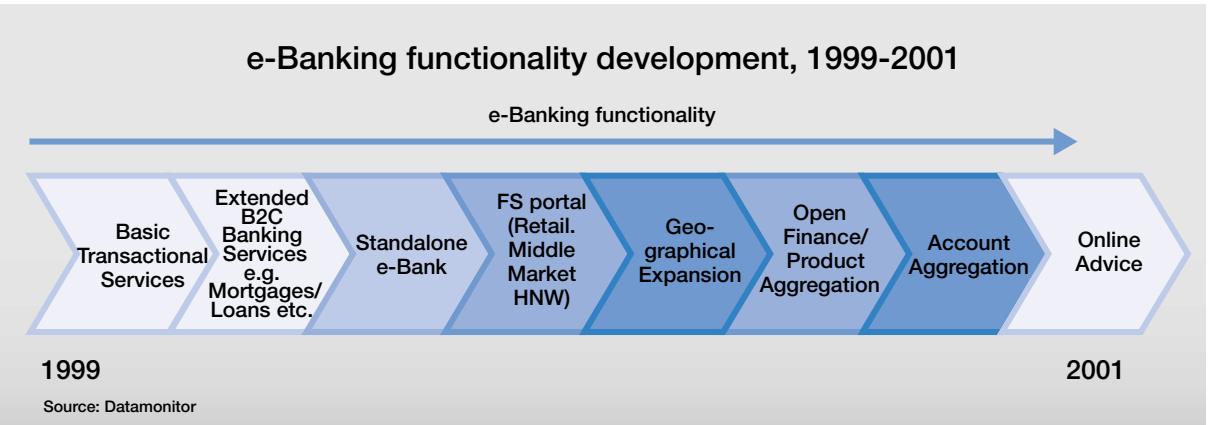

Figure 1

Mobile devices and consumers

The market for consumer mobile applications brings with it a greater number of challenges than corporate uses. For example, customers are likely to connect to a service using a variety of different devices with differing interfaces and operating systems. Variations in the quality of connectivity offered by different telecoms providers will also impact how well a service is perceived.

Like e-Commerce and e-Banking, consumer-based mobile applications also have to be scalable, to cope with unpredictable demand. Security is another major consideration, both for business and consumer-based applications. Frailties in early wireless protocols deterred many consumers from adopting m-Banking services, and high-profile problems in the early days of e-Banking have also made consumers cautious about using self-service banking channels.

Current Technology Barriers

Although many banks and retail organisations have already begun to experiment with using mobile devices to deliver financial services, there have been a number of limitations in the past that have hindered the take-up of m-Finance and m-Banking services.

Handset capabilities

WAP enabled mobile phones began to emerge in late 1999. However, many of these early devices offered small, monochrome screens that were poorly optimised for displaying more than a few characters of data. Additionally, WAP data presentation was handled differently by each handset manufacturer, meaning that information was displayed differently on each phone. In order to support all WAP devices, service providers had to create a modified version of their content for each individual phone.

Other problems encountered by WAP included security. Early versions of the WTLS (Wireless Transport Layer Security), responsible for managing the security of data, had a number of shortcomings, which meant that WAP wasn't really suitable for transactional use, or for transfer of critical data.

Types of device

Mobile phones and PDAs are currently two of the options available for delivering wireless services, but in the future, this device market will diversify to include smart phones, in-car devices and other forms of receiver. At present, mobile phones are characterised as low-cost, widely available devices that offer limited functionality and no local processing power. In contrast, PDAs offer far broader functionality, but currently lack the same degree of wireless connectivity as mobile phones. The PDA market also suffers from incompatibilities between applications and operating systems, making development difficult.

Network Limitations

Widespread use of GSM (Global System for Mobile) has meant that Europe already has a strong digital mobile phone user base. However, GSM is hampered by slow data transfer speeds and limited functionality. This strong consumer interest makes Europe ideally placed to take advantage of some of the new opportunities offered by faster wireless technologies such as GPRS (General Packet Radio System) and UMTS (Universal Mobile Telecommunications System). GPRS and UMTS also use packed switch technologies, rather than circuit switching which is used for GSM. This is likely to change services and applications dramatically, by offering always-on connectivity.

Many of the limitations of current m-Finance and m-Commerce applications are as a result of slow network speeds, so these improvements will be of significant benefit in this industry. The following table shows a comparison between data transfer rates for the most common wireless communication services:

Standard	Maximum data transfer rate	Availability
GSM	9.6 Kbps	Current standard in Europe
HSCSD	14.4 Kbps	Available now, although little used
GPRS	114 Kbps	Emerging
EDGE	384 Kbps	Expected in 2002
UMTS	2Mbps	Expected in 2004

UMTS is considered to be the only 'true' 3G network service in this table. Services like GPRS and EDGE provide some elements of 3G functionality, such as always-on capabilities, but fail to offer sufficient bandwidth for 3G-style applications.

However, both EDGE and GPRS may well be fast enough for many consumer applications, and both standards are likely to offer a cheaper alternative to UMTS. This means that m-Finance and m-Commerce can become a reality in the near future, rather than having to wait for UMTS availability.

Defining suitable applications

It has taken some time to identify suitable services for wireless devices. These must deliver genuine added value, while taking into account some of the current limitations of mobile technology.

Organisations such as banks and e-Commerce ventures have been at the forefront in developing new mobile services. For an organisation with an existing web site, adding WAP functionality doesn't demand major financial investment, as it only requires a gateway to convert HTML content to WML format. However, there are broader implications in ensuring data is secure over a wireless network and that it is presented in a form suitable for a mobile device.

The always-on nature of GPRS networks and similar wireless standards opens up a far wider range of possibilities. There's the potential to guide customers to their nearest cash point, for example, or to provide up-to-the-minute information on share performance. Further consumer applications, such as multi-player gaming are also likely to be success stories from new wireless networks.

Changing the Way We Work – New Business Requirements

Changes to Current Working Methods

Faster network services like GPRS, coupled with more powerful mobile handsets, will create opportunities for many new services. This applies both within the workplace and in the consumer field.

Financial services in particular stand to benefit from these innovations. New payment methods and collaborative ventures with other industries are two examples of potential wireless services. However, this broader functionality also brings with it an increased need for robust security and manageability.

New payment methods

Micropayments

Micropayments, or digital cash, are already beginning to emerge in the e-Commerce world. These address small value purchases, such as buying a single MP3 track from a web site, and can be passed from consumer to consumer, instead of through a bank. The units involved are also generally too small for a credit card transaction.

Digital cash units can be stored on a smart card or other removable device. As payments are made, the stored units decrease. These can be topped up via a suitable machine, or through a card reader attached to a PC. In the wireless market 'm-Cash' could be stored on a suitable SIM card, or on a smart card that could be used in conjunction with the handset.

Macropayments

It's anticipated that the market for m-Cash will remain relatively small in the future. The need to manage payment units on a separate card may deter many consumers. However, for mobile finance, macropayments show much greater potential. Use of macropayments mirrors existing credit card use, in that a single identification method is used for all of a customer's transactions.

A digital wallet, stored on a mobile device or on a removable card, holds details about the customer, such as a bank account or credit card number. It then enables them to make a payment online based on these details. Instead of having to register for multiple finance or commerce services individually, the user signs up once with a single digital wallet provider.

An Increased Need for Security

As consumers begin to use mobile devices for a wider range of tasks, the need to ensure that data remains safe, both on the device itself and while in transit, will also increase. The always-on nature of 3G networks means that there will be a continuous security risk whenever a user is connected to the network.

There are four main requirements for mobile security:

- Confidentiality – transactions and other types of data must remain private
- Authentication – the message sender must be known to the merchant or bank, and must be identifiable
- Integrity – data must not be altered in transit
- Non-repudiation – transactions must be legally binding

Data encryption, digital certificates and digital signatures are three of the major technologies that are currently emerging to support these requirements.

- Data encryption – information is converted into an unintelligible format. It can only be re-converted into a legible form using appropriate identification.
- Digital certificates – these are digitally stored documents that contain information about a user. Their contents must be guaranteed by a trustworthy Certificate Authority. Banks can act as a Certificate Authority.
- - a digital signature uniquely identifies an individual, and is used in data encryption processes such as PKI (Public Key Infrastructure). The ability to perform a digital signature can be protected using a password, a passphrase, or another form of identification, such as a digitally stored fingerprint.

Better Manageability

Even with the greater bandwidth available from GPRS or UMTS, network limitations are still likely to cause problems in the short term. As greater numbers of consumers take up services, wireless network capabilities are likely to become stretched. This will be particularly apparent if multimedia applications such as streaming video begin to gain wide support. As a result, manageability will remain an issue, both within corporate wireless networks, and across public WANs. Bandwidth priorities may need to be considered by wireless operators. Handset developers will also need to build greater local processing power into devices in order to reduce the data transfer overheads required from the network.

New Technical Requirements

As the requirements of m-Commerce and m-Finance increase, a new processor architecture will be required to handle these demands. This architecture needs to be capable of handling high levels of data transfer, as well as providing local processing power for wireless applications. It must also provide a secure environment in which to carry out mobile transactions.

Both mobile workers and consumers will have similar demands when it comes to being able to carry out tasks quickly and efficiently. However, the potential problems caused by poor security or limited processing capabilities will be more apparent in consumer applications.

Intel® Personal Internet Client Architecture

Problems of the past

Reducing the form factor and power consumption of mobile devices has been an ongoing challenge for chip designers. Traditionally, mobile phones have used DSPs (Digital Signal Processors). These are only capable of running at low clock speeds, limiting their processing power. However, they still demand significant amounts of battery power in order to run effectively.

To create a complete chipset for a traditional mobile device, developers also had to incorporate a separate microprocessor and memory modules into their designs. This added complexity to the chipset, and made devices difficult to program.

A solution for the future

The Intel® Personal Internet Client Architecture addresses these problems by enabling a standard applications platform built around a general-purpose microprocessor, defining an open environment for hardware and software development yet allowing connection to a wide variety of wireless interfaces. The Intel® PCA partitions the device configuration of the traditional cellular platform into: an Applications Subsystem, Communication Subsystem, and Memory Subsystem. This partitioning allows application development to evolve independently from communication standards. By defining a hardware architecture with common components and open interfaces, and providing a software framework with open interfaces and services, device and application developers can design, scale, and broadly deploy their products with less cost and in shorter time.

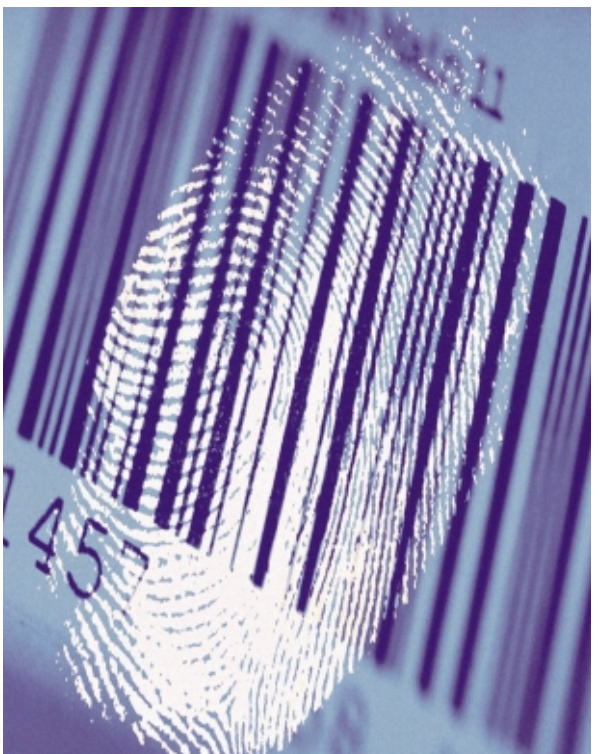

Figure 2 below shows the general design of the chipset:

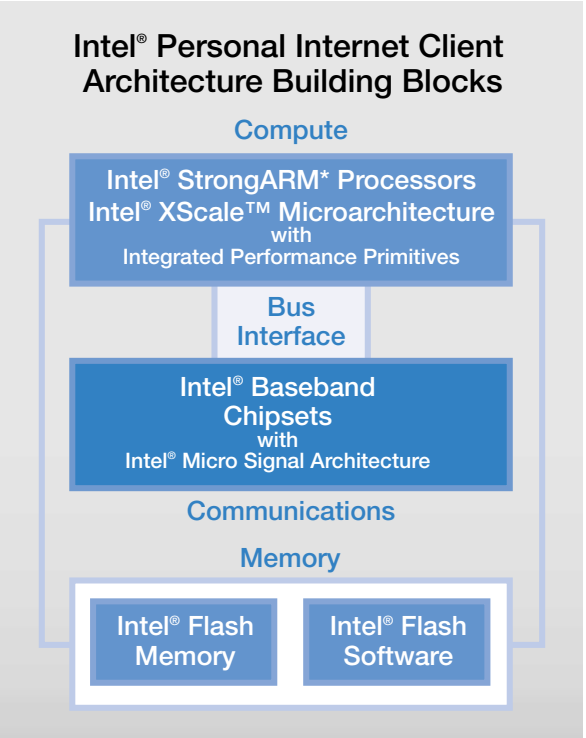

Figure 2

Applications Subsystem

Intel supplies high performance yet low power building blocks for the Intel® PCA Applications Subsystem. The current StrongARM processors already power high performing PDAs such as Compaq iPAQ and also some 3G cell phones coming out in Japan. The next generation application processors based on Intel® Xscale™ microarchitecture will further progress the high performance and low power capabilities.

Communication Subsystem

The Communication Subsystem provides the services to access cellular wireless networks and Intel's building blocks for this subsystem are based an easily-programmable Intel® Micro Signal Architecture (Intel ® MSA). A DSP with micro-controller features, Intel® MSA based building blocks enable high-level language programming and also small, ultra low-power wireless devices.

Memory Subsystem

A major component of the Intel® PCA is the memory subsystem and Intel® has been a leading vendor for industry-leading Flash memory solutions for cellular and wireless applications. By also providing leading edge software solutions such as Intel® Flash Data Integrator (Intel® FDI), Intel reduces development time significantly while increasing performance at the same time.

The software architecture of Intel® PCA takes an open approach, supporting three different types of application

- Native Embedded – binary-code based applications that are added to the chip at the time of manufacture
- Native Downloaded – binary-code based applications that are installed by the user
- Applications – developed in languages such as WML or Java. These add functionality and deliver extra value to devices. In higher level uses such as m-Banking and m-Commerce, this layer of development is essential, enabling banks or vendors to create their own applications for these devices.

A scalable, flexible solution

As the Intel® PCA hardware architecture is also open, it's possible for handset developers to create highly scalable solutions, by combining PCA modules in different ways to create custom devices. Separating communication and computing functions also assists scalability, by enabling developers to add extra features at a computing level, without affecting communications.

This also offers other advantages to handset designers. A family of devices can be created from a single development effort, and interchangeable peripherals such as wireless modems can also be added into handsets as required. A single device can be shipped worldwide due to Intel® PCA support for multiple air interfaces, requiring minimal localisation. Manufacturers will only need to change features such as the wireless modem, without having to alter the architecture or application design.

Intel® PCA in action – the Compaq* iPAQ*

Compaq offers two new platforms of the iPAQ Pocket PC family - the H3700 and H3800 Series – the ultimate blend of performance, connectivity and expandability to meet the widest range of handheld computing customer needs.

The new Handheld platforms are based on the new Microsoft Pocket PC 2002 OS, feature the design of the original iPAQ Pocket PC and incorporate the fastest processor available, the Intel® StrongArm 206MHz. The Compaq iPAQ H3800 Series offers an integrated Secure Digital (SD) slot for internal (memory) expansion, a good quality TFT screen supporting 65K colours and increased battery life. The high-model also incorporates integrated Bluetooth technology, supporting personal area network capabilities. The Compaq iPAQ H3700 Series preserves the outstanding feature set of the Compaq iPAQ H3600 Series, while incorporating 32MB ROM, 64MB RAM and leveraging the new Microsoft Pocket PC 2002. Next to that, both Handheld platforms offer a set of Compaq specific applications like iPAQ File Store, iPAQ Task Manager and the ViaVoice Mobility suite for voice command and control.

From a wireless client perspective, Compaq has presence within Personal Area Network (PAN), Local Area Network (LAN) and Wide Area Network (WAN) environments. In the PAN area, Compaq has the new Bluetooth Wireless Pack with CompactFlash (CF) for the Compaq iPAQ H3600/3700 Series, offering PAN capabilities (with BT-enabled phones, printers and Compaq notebooks through the Compaq Mulitport technology). Compaq also offers an uniquely integrated BT-offering in the high-end Compaq iPAQ H3800 Series. In the LAN environment, there is a broad range of wireless client devices (for instance PC Cards, Wireless USB) and wireless access points for the mobile platform offering. In the WAN, Compaq recently launched the Wireless Pack for GSM/GPRS networks, transforming the Compaq iPAQ product into a wireless PDA, enabling high-speed Internet access, wireless e-mail, SMS, support for GSM calls throughout the world and supporting data services through GPRS technology.

Blueice* Multipass* – Wireless Security

Improved handset design, through the use of Intel® PCA will provide much greater flexibility for designers of services such as m-Finance. However, with increased functionality there comes a greater need for security. Blueice Research Multipass Client and Server modules can add this important element to a wireless solution. The use of the free, downloadable Client in conjunction with the Server's functionality provides a robust end-to-end security solution.

Multipass Client

The Multipass Client is both an offline and online product. In offline mode, the client enables sensitive data to be encrypted and stored on a mobile device or PC. This means that, should the device be stolen, all stored data will be inaccessible to anyone without the necessary identification. When the mobile device connects to a network, digital credentials such as private keys, which are stored in the secure storage area, can be used by the Multipass Client when performing security transactions with a transaction server.

When a customer first uses the Multipass Client, they are required to enter their security details. A triple DES (Data Encryption Standard) key is generated. All data stored in the Multipass database is encrypted with this key. The user also has to choose a passphrase. This passphrase is used to encrypt the triple DES key that is used to encrypt the data

Typical data that might be encrypted in this way includes personal information, such as an address or telephone number. It is also used for 'digital credentials' including data like credit card numbers, or passwords for secured sites.

This forms part of a PKI (Public Key Infrastructure) function.

PKI offers a powerful form of encryption, and is now being adopted by many organisations who need to ensure that their users' data remains safe. In general, encryption converts readable materials such as text or numerical data into an illegible string of characters, using an encryption key. To convert the character string back into legible text again, a second key is used to 'unlock' the data.

Traditional methods of encryption were termed 'symmetric encryption'. This approach required both the sender and recipient of the encrypted data (such as a bank and a customer) to share the same secret, or 'key', in order to lock and unlock data. However, PKI uses asymmetric encryption, a more secure and complex form of cryptography. Asymmetric encryption uses a 'key-pair', comprising a public and private key. In an m-Banking scenario, the public key would be held by the bank, and distributed to all customers who wish to use its m-Banking service. A unique private key is created separately by each customer, and is known only to that individual. One part of the key pair is used to encrypt data, and the other to decrypt it, ensuring that only the intended recipient can view the information. This process is shown in Figure 3.

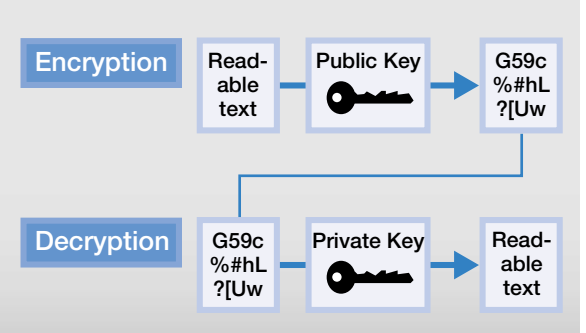

Figure 3

Within the Multipass Client solution, the relevant public key is submitted, via the Multipass Server, for signing by a Certificate Authority (CA)."

Cross platform support

The Multipass Client supports cross-platform security, and is compatible with the following operating systems:

Mobile operating systems:

- Palm* OS 3.5 and above,
- Windows CE* 3.0, Pocket PC 2000*
- EPOC* 32 R6 and higher

Desktop operating systems:

- Windows NT* 4.0,
- Windows 2000*
- Windows 95*/98*/ME*

It is also capable of supporting multiple browsers for online work. The major browsers supported are:

- Microsoft* Internet Explorer* 4.0 or above
- Netscape* Navigator* 4.0 and above
- AvantGo* 3.3 and above

Multipass Client architecture

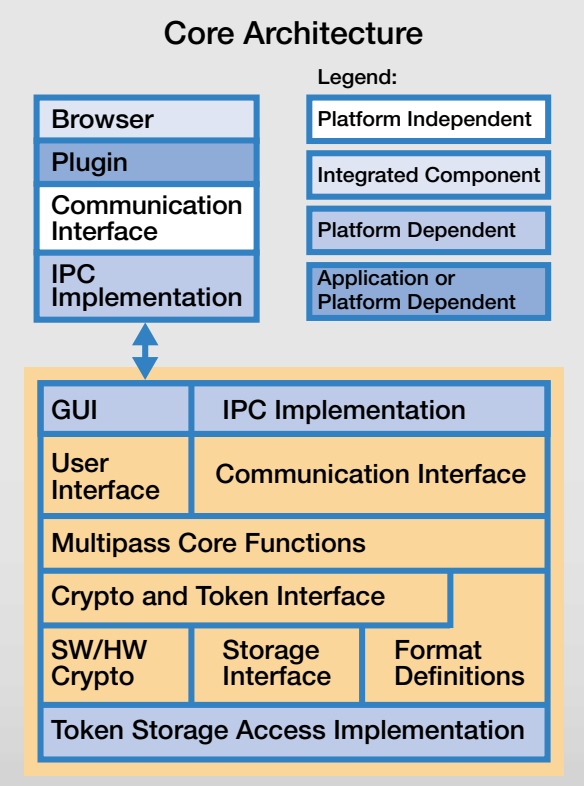

Figure 4

The Multipass Client has a layered architecture. The core elements of this, highlighted in Figure 4, provide the Client's main functionality. Some of the core security components of this include:

- User Interface – this is comprised of two main folders, a Personal folder that contains encrypted private information, and an online Services folder for storing encrypted information required to use m-Finance or m-Commerce applications.
- Crypto and Token Interface – this uses an internal API that supports the use of tokens such as smart cards for identification. In this instance, the certificates and private keys required to use online services are stored on the token itself. As this is included as a separate module, it makes the process of updating the Crypto and Token Interface straightforward. This is important as new smart card standards are still evolving.
- Storage Interface – an independent API is used for storage. This is a platform independent interface, making it easy to adapt the client to any operating system or storage requirement.

Figure 5 shows how the Multipass Client is structured. The user can access their Personal and Services folders once they have logged into the system using their passphrase.

The Client also contains other functions, such as:

- Changing passphrase
- Customising the appearance of information in the Personal folder
- Specifying when the Client should lock information – for example, locking can be initiated after a specified length of time if the Client is left unused, or if the program is terminated.

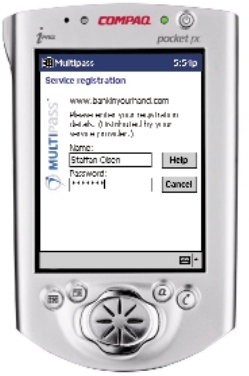

Figure 6

The interface for user logon (shown in Figure 6), simply requires a username and passphrase. The user's PKI credentials are verified by the Multipass Server. The communication between the Multipass Client and Server is conducted over SSL

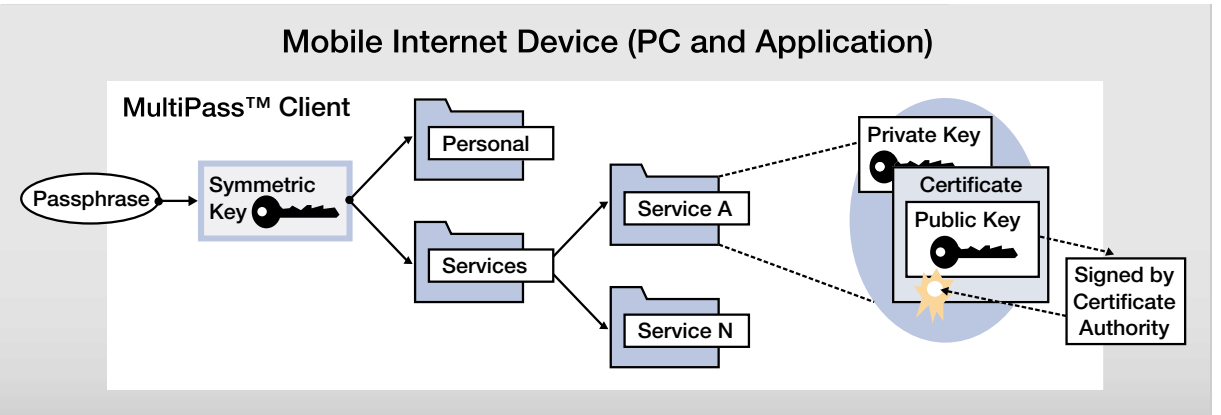

Figure 5

Communication with a browser

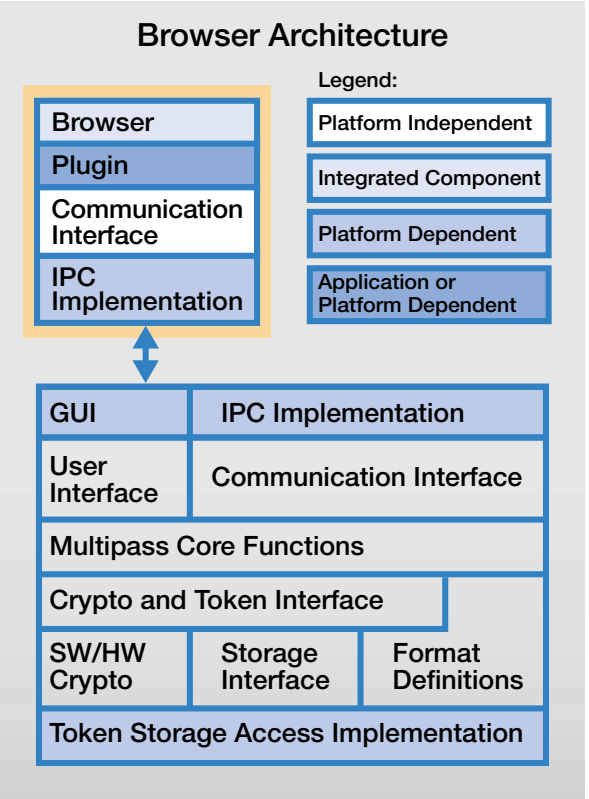

Figure 7

The plug-in components of the Multipass Client architecture, highlighted in Figure 7, manage browser operability. Each browser type requires a different plug-in. In the case of Internet Explorer*, this is an ActiveX* control, but other browser types have unique requirements. The Multipass Client also contains an API interface that allows applications, that do not have a plug-in mechanism, to make use of Multipass Client's security functionality.

Communications between the browser plug-in and the underlying Multipass Client architecture are also managed differently, depending on the operating system in use. The three major methods are:

- COM* (Component Object Model) – this is used with all Microsoft* Win32 platforms, such as Windows* 95*, 98*, ME*, NT* and 2000*.
- Shared Memory – this technique is used with Windows* CE* Devices
- The Palm* OS only allows a single application to run at any time, so information is stored by Multipass Client until it is required.

Multipass Server

The Multipass Client only forms one half of Blueice Research's solution. The Multipass Server supports site registration, authentication and digital signatures. It can also issue digital receipts on behalf of an organisation.

This operates using the same PKI system as the Client element, offering an end-to-end security solution. Multipass Server also supports a wide range of standards and protocols. It is Certificate Authority (CA)-independent and can be deployed by any network operator, for use with a wide variety of communication protocols.

Multipass Server can be used in conjunction with existing online applications, making implementation straightforward.

Simple registration

When a user enters his or her identification details via the Multipass Client, the Multipass Server will retrieve user information based on the authentication from an external database. This data is then sent with the user's public key from the Multipass Client, via the Multipass Server, to the CA for signing.

As shown in Figure 8, a mobile device such as a smart phone or PDA can be connected to the Multipass Server application via a wireless data network. The web server-based application uses data from Multipass Server to retrieve information from service applications and CAs.

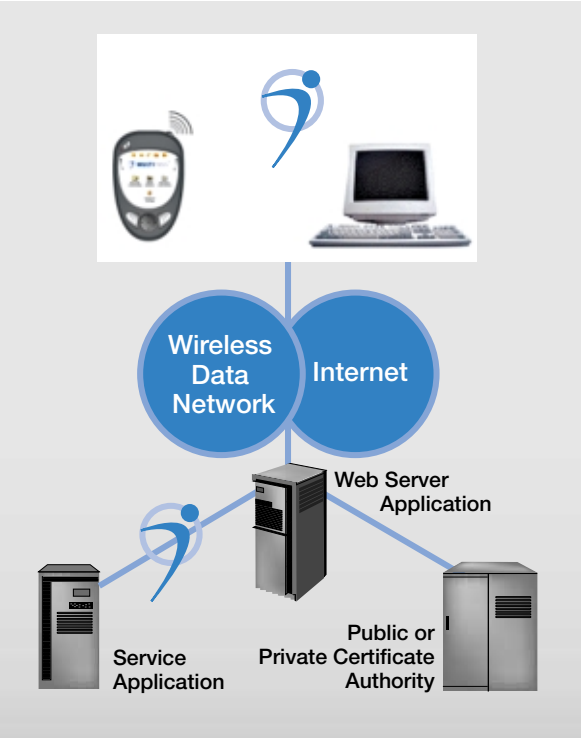

Figure 8

Server architecture

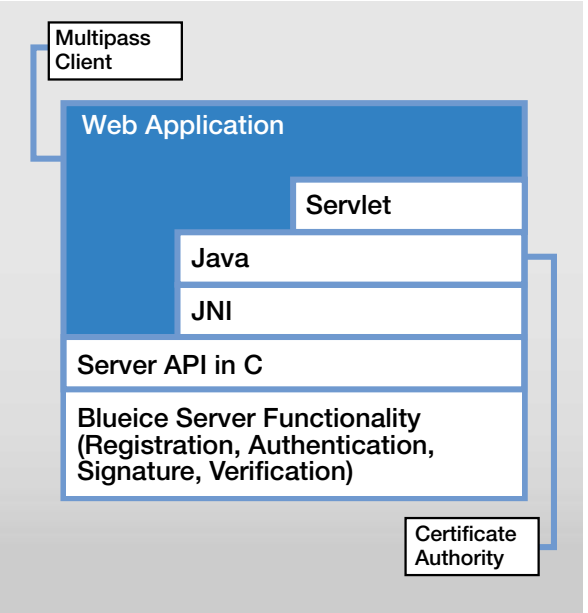

Figure 9

The Multipass Server architecture is designed to be used in conjunction with web-based applications. Both a servlet API and Java or C/C++ API are supported, making this a flexible solution for web developers.

Communication between the Multipass Client and the Multipass Server is managed using HTT commands, a standard for web-based communications. The following triggers are recognised by the system:

- Register – register a new user
- Authenticate – authenticate an existing user
- Sign – perform a digital signature
- Digital receipts - issue a digitally signed receipt
- Logout – terminate a user session.

Scalability, reliability and availability

Multipass Server processing is carried out at the web server level. The architecture is designed so that if required the server can be run either on a single host, or on multiple machines in parallel.

Intel® Pentium® III Xeon™ processors, together with the Multipass Server, provide a simple, cost effective method of ensuring high scalability. Extra machines can be added at the web server level as required, and each machine can include a Multipass Server ensuring fault tolerance, load balancing, and high availability, while taking advantage of the core benefits of the Intel® architecture. As the Multipass Server will be required to process varying levels of traffic securely and efficiently, ensuring that there are no bottlenecks in the system and eliminating a single point of failure are both essential requirements. The power available from multiple single Intel® Pentium® III Xeon™ processor machines, used in conjunction with a load-balancing application, can ensure that systems remain reliable offering cost-effective and outstanding performance.

The strong multiprocessor capabilities of the Intel® Pentium® III Xeon™ processor also offer exceptional support for scaling up. The Intel® Pentium® III Xeon™ processor technology provides granular scalability, meaning that additional processors can be added as required to create 4-way or 8-way systems, up to a maximum of 64 processors within a single machine. Combined with strong reliability and manageability features, scaling-up using the Intel® Pentium® III Xeon™ processor provides a means of consolidating systems, boosting performance and conserving floor space.

Whether scaled-up or scaled-out, the Intel® Pentium® III Xeon™ processor offers powerful availability features, including functional redundancy checking and a dedicated system management bus. For scaled-up 4-way or 8-way systems, additional features such as hot swappable and redundant subsystems, automatic failover technologies and failure prediction ensure that systems remain available and reliable at all times.

Infovention* Transigo*

Bank-in-your-Hand's core applications have been implemented using Infovention's Transigo framework. This architecture provides both outstanding performance and a solution that is flexible enough to respond quickly to market changes.

It enables different back-end applications and third party products to be integrated seamlessly, providing banks with the ability to build tailor-made solutions that add value to customers. The architecture is Java 2 Enterprise Edition (J2EE) compliant which enables delivery of a number of core application features:

- Multi-channel access to business logic – This means that a customer should be able to access application services through several different devices and/or media. Using technologies such as SMS messaging and WAP for banking add to traditional channels such as ATMs or the telephone. It is important that an architecture is flexible enough to easily incorporate new channels.

- Personalised content, processes and communication – Personalising look and feel, communications and marketing campaigns all enable banks to deliver a more focused service to each customer.
- Transactional business logic – Using J2EE components to deliver transactional business logic reflects the processes that have been carried out for years using older methods such as CICs or Tuxedo. ACID properties (Atomic, Consistent, Isolated and Durable) should be adhered to when moving the application to a new platform.
- Flexible security policies – A flexible system should enable multiple authentication methods, such as username/password or use of digital certificates. Supporting access control policies based on user identity, authentication method or the channel being used is also important. Dynamic activation and deactivation of resources and services is another element of security provided by Transigo*.
- Integration with legacy systems – Integration of older IT systems involves both technical issues, such as supporting the computer platform, network protocol and implementation language in use, and functional issues like data formats and attribute naming.
- Reliability, Availability and Scalability – Designing software to take advantage of the hardware capabilities provided by the Intel® Architecture is another important consideration.

Transigo* Architecture

The architecture for the Bank in your Hand application uses the following general architecture

Business Benefits

Multipass*, Infovention and Intel® PCA in Action

Blueice Research, Infovention and Intel have contributed their technologies towards the first complete mobile finance solution, offering a fast, safe service for consumer banking. *Bank-in-your-Hand* combines the end-to-end security offered by Multipass with the power and scalability of Intel® PCA infrastructure.

Security is of paramount importance in the banking industry. To address this, *Bank-in-your-Hand* combines the Multipass solution with Intel® PCA to create a unique system, offering robust data protection not available from any other technology. Personal data can be stored within the components of Intel® PCA and encrypted using Multipass. If a consumer loses a handheld device, their banking data will remain safe. However, when they need to contact their bank, either to carry out a transaction or to request information, the wireless power of Intel® PCA will enable them to connect from anywhere on a GPRS or WLAN network.

The *Bank-in-your-Hand* project has been carried out in conjunction with Compaq, using the iPAQ Pocket PC. This is based around an Intel® StrongARM* processor and offers 802.11b Wireless LAN support, as well as GPRS capabilities. Ease of use has also been important in creating the application, making it accessible to as wide a consumer audience as possible.

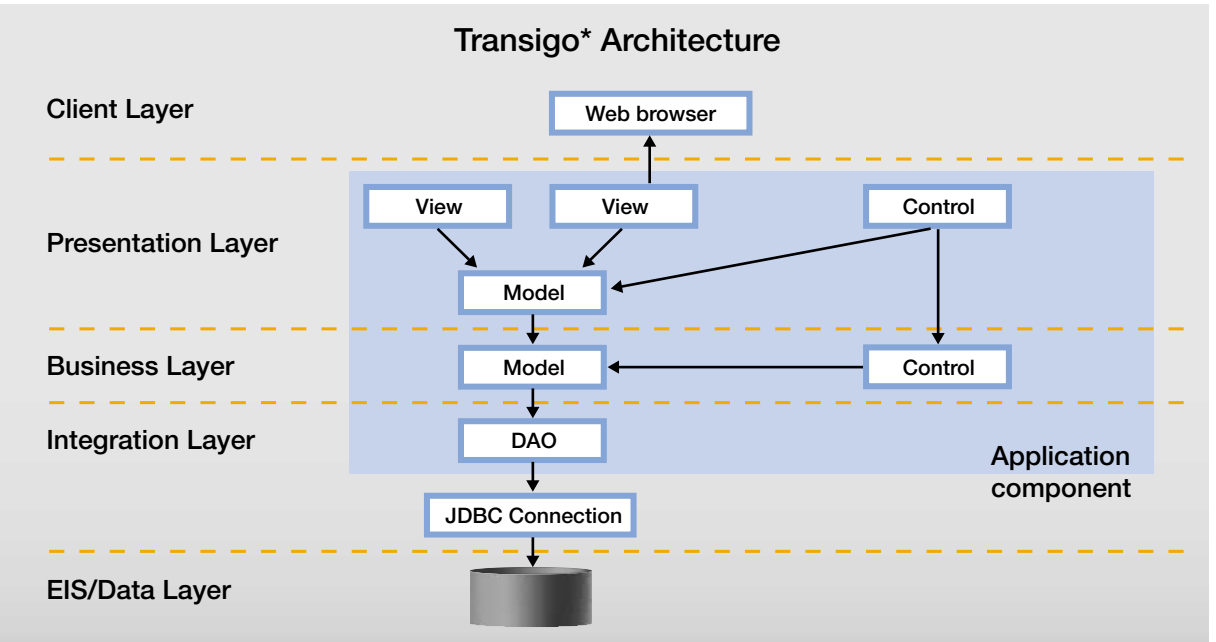

Figure 10 – Transigo architecture

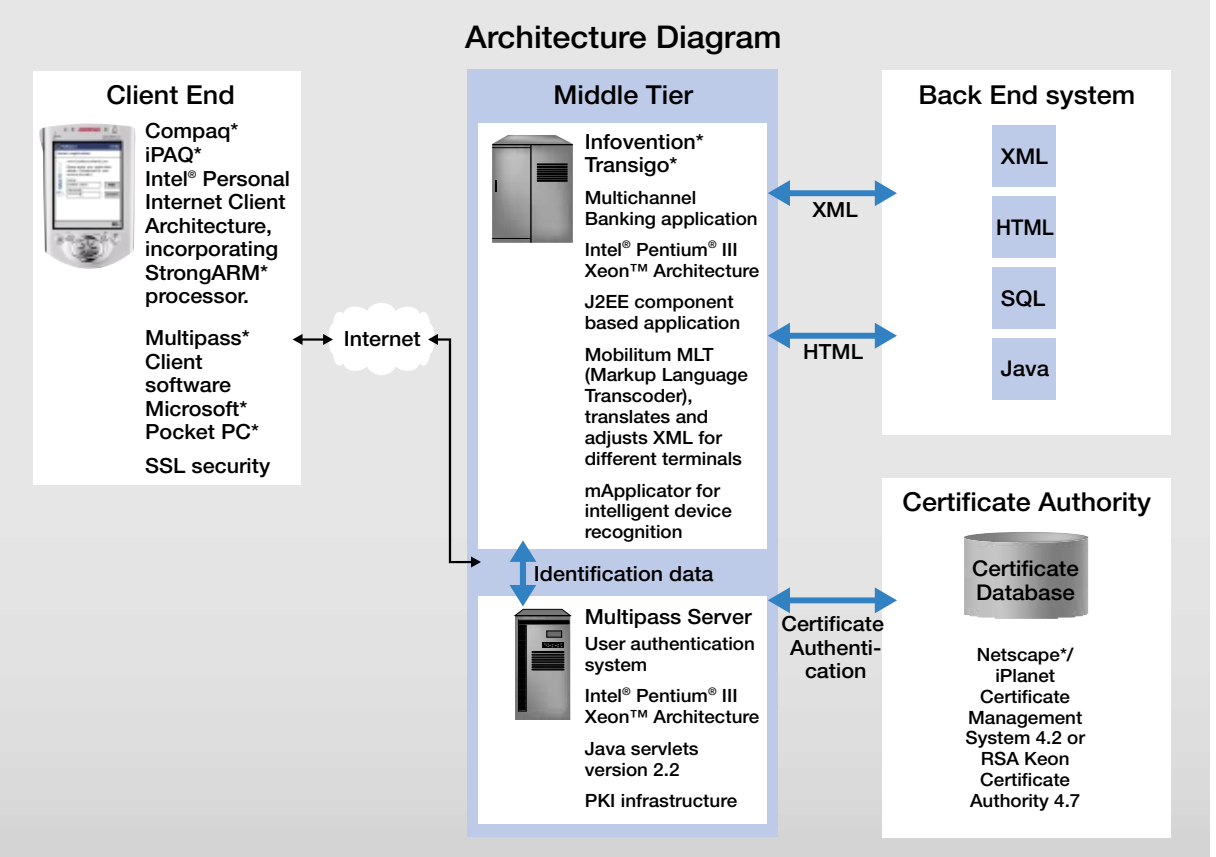

Figure 11

Figure 11 shows how these elements have been combined to create the *Bank-in-your-Hand* solution:

Secure, cost-effective m-Banking

The *Bank-in-your-Hand* solution eliminates the need for end users to carry both a mobile phone and an additional form of electronic identification in order to use their m-Banking service. Providing tokens such as smart cards, that can act as electronic identification, is a costly undertaking for banks. It also introduces added complexity for a bank's m-Banking customers. However, through the use of Intel® PCA and Multipass, *Bank-in-your-Hand* provides both a browser and a security device on a single machine, offering a more convenient and cost-effective solution for banks and end users.

Once users have signed up for a mobile banking service, through the Multipass Client and Server solution, they can then use their device for a variety of different banking functions, including:

- Bank account overviews and more detailed information on specific items within their account
- Electronic bill payments
- Intra-and inter-bank transfers
- Overview of scheduled payments.

Combining technologies for an end to end solution

Bank-in-your-Hand makes the most of both Intel® PCA, the Multipass Solution and Transigo's flexible banking capabilities. Intel® PCAs modular chipset means that developers such as Compaq can devise powerful devices offering a robust architecture for m-Banking. As well as enabling efficient wireless Internet access, Intel® PCA also offers the benefits of CPU processing power, expandable memory and long battery life. This means that processes such as PKI key generation required by the Multipass Client can be carried out on a handheld device, rather than through a PC. As a result, a PDA or mobile phone becomes a complete mobile banking solution, rather than an add-on to an e-Banking or PC-based solution.

The previous generation of mobile phones lacked the processing power required for client registration and the memory capacity for storing digital certificates. However, the Intel® PCA modular architecture provides device developers with the ability to add potentially limitless storage to a device. This will reduce the need to store digital certificates on smart cards or other forms of hardware token.

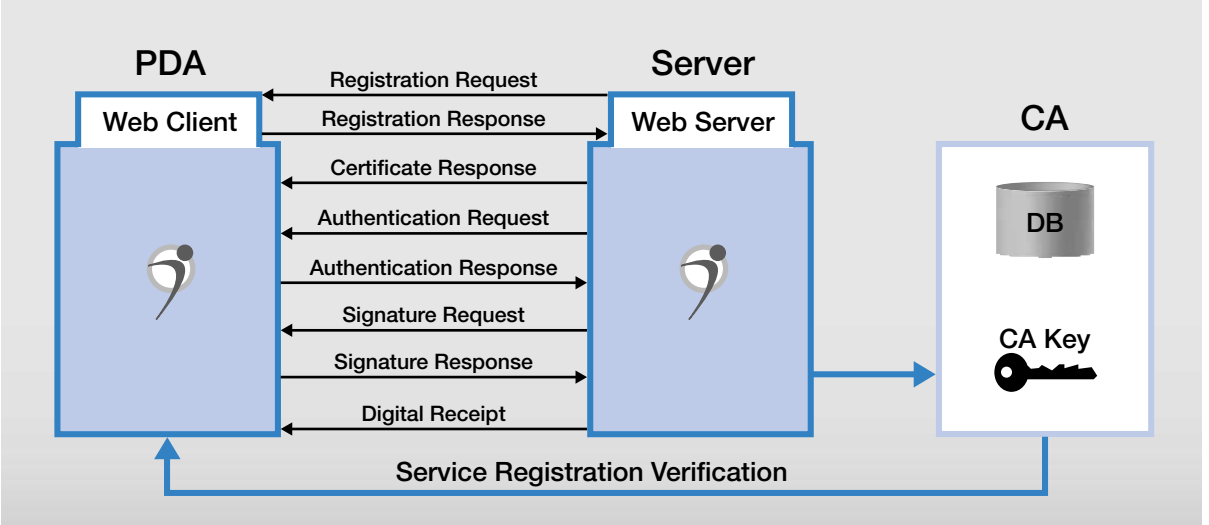

Figure 12

Figure 12 shows how data flows between an Intel® PCA device and the Multipass Server within *Bank-in-your-Hand.*

The wide support of the Intel® PCA for air interfaces and wireless standards also makes the Bank in your Hand solution highly flexible. The solution can be deployed by financial institutions anywhere in the world, with little need for customisation.

Bank-in-your-Hand also makes use of the benefits of the Intel® architecture for back end processing. Web server hardware, incorporating Intel® Pentium® III or Xeon™ processors, can be used in conjunction with the Infovention Transigo server software that supplies the middleware layer for *Bank-in-your-Hand*. Transigo provides a framework of J2EE components capable of taking advantage of the scalability and reliability features offered by the Intel® architecture, such as hot swapping and fail-over.

The Future

Bank-in-your-Hand is evidence of how the Intel® PCA structure, Blueice Research Multipass and Infovention Transigo can be used together alongside third party products to create innovative and flexible solutions. This early application is dedicated to banking, but in the future, similar products could be constructed for other industries, such as general commerce sites, or entertainment networks.

As PDA and smart phone manufacturers begin to build on the capabilities of Intel® PCA to create new, powerful devices, the processing power available to application designers will increase. The ability to divide tasks between a server and a wireless client will mean that features such as multimedia use will also become a reality. For example, compressed, encrypted video files can be passed over a GPRS or 3G network, then processed by the client device for viewing locally.

As the Multipass Client and Server can be branded to fit the requirements of any organisation, there are also opportunities to customise the service to any business needs. With free, downloadable Multipass Clients available from Blueice Research, this makes Multipass a highly flexible and cost-effective solution to the problems of data security. In addition, the flexibility of the Infovention Transigo platform enables banks to provide unique services that can be tailored to individual customers.

Produced by Intel EMEA Marketing Programs & Alliances,
Vertical Industry Marketing Group
and Technical Marketing.