

# NonStop Goes Mobile

**Juergen Depping**  
CommitWork GmbH

Juergen is one of three founders of CommitWork in 1997. CommitWork is doing project business with several German NonStop manufacturing customers, is providing application framework- and software development products and since 1999 focusing on the usage of Java on HP NonStop.

**E**nterprise users must start connecting Smartphones and Tablets to HP NonStop, an important step as BYOD (Bringing Your Own Device) is challenging Corporate IT by bringing and integrating privately owned user devices into enterprise networks. It is an extreme of utilizing mobile devices: completely open and not very much control. Most enterprises will probably decide for only allowing their own mobile devices to better control apps and settings used on these devices. Despite all security discussions, banks for instance have already brought Internet banking apps

on Smartphones into this arena. So time seems now to be ready for using these devices also in connection with Intranet based applications.

Imagine a scenario where you are getting informed by your Credit Card provider that your Credit Card is used right now in Shanghai for purchasing high value goods. The Credit Card provider is internally using fraud detection algorithms for finding deviations from your usage pattern and you had accepted a subscription for using such a fraud information service and you are now embedded in a "fraud detection loop" with your Credit Card provider. If you

indeed travelled to Shanghai for the first time, you can have a good feeling that fraud detection is working, and if not, you instantly can get ready to become active.

This scenario is not Intranet based from the Credit Card provider's point of view. Risk, getting caught by any kind of spyware, today is mostly on the user's behalf. Internet usage sets different rules. Therefore more efficient security tools on Smartphones and Tablets are and will be available to enable utilizing these devices also within enterprises' Intranets.

Forbes Magazine reported in their article in October 2012 "Top 100 iPad Rollouts by Enterprises & Schools" ranked by number of devices. Indeed, nearly 70 out of the top 100 list were schools and universities. But the list of 100 is headed by Korea Telecom using 32.000 devices. They come from firms/organizations like US Air Force, SAP AG, Roche (healthcare), Cisco, United Airline, IBM, Singapore Military, Royal Caribbean (cruise lines), Sears Holdings, Air France, Verizon, British Airways, General Electric, Hyundai, La Guardia Airport and Walt Disney. Belonging to the top 50 in this ranking, they use a minimum of 2000 iPads in their deployments.

In March 2011 Gartner Group already provided a study "iPad and Beyond: The Media Tablet in Business". Their key findings were: "Media tablets present a variety

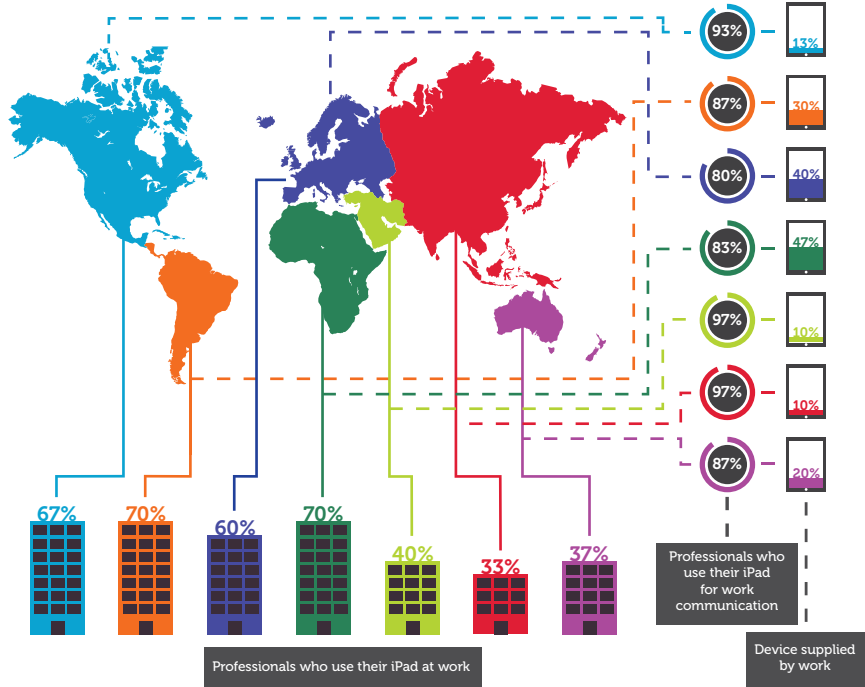
- iPad for Business Survey
- Infographic Summary
- Introduction
- Rival Devices
- Content Consumption
- Business Tool
- Location & Connection
- Purchasing & Satisfaction
- Continent Case Studies
- Africa
- Asia
- Australia / New Zealand
- Europe
- Middle East
- North America
- South America
- Conclusion

IDG Connect is the demand generation division of International Data Group (IDG), the world's largest technology media company. Established in 2005, it utilises access to 35 million business decision makers' details to unite technology marketers with relevant targets from any country in the world. Committed to engaging a disparate global IT audience with truly localised messaging, IDG Connect also publishes market specific thought leadership papers on behalf of its clients, and produces research for B2B marketers worldwide.

For more information visit:  
<http://www.idgconnect.com/>



## iPad use at Work



Pic. 1: Source: January 2012

of new opportunities for business, while supplementing traditional uses of notebooks and Smartphones. Tablets present a new design point for applications, and require a new set of policies, technologies and skills". Gartner Group encouraged enterprises to provide custom built apps on iPhones and iPads for Intranet usage, but they also said, these new technologies require new skills, new tools and new concepts in the areas of managing enterprise networks and developing apps for enterprises.

In January 2012 IDG Connect published their "iPad for Business Survey 2012" stating that usage of iPads for work related tasks is increasing heavily. 10% of business users worldwide say they have replaced their laptops completely by iPads and 50% say they have replaced them partly. (Pic. 1)

It seems to be clear that this fast growing usage of Smartphones and Tablets will have a severe impact also on enterprise communities. Whether firms and organizations purchase those devices for their employees or they let them use their privately owned devices for business tasks (probably in both cases an enterprise can save lots of money), usage will jump over from Internet accessing, mail, text and spreadsheet applications on mobile devices to Intranet-like applications: no one will understand that he or she should be running around using two devices for different tasks. This demand will push the mobile device makers and the security products industry to provide appropriate functions and tools soon – if not already available.

Since more than 35 years, the outstanding features of HP NonStop systems are the main reasons for many enterprises, to deploy their most critical applications onto these servers. Applications like Credit Card transactions, HLR (Home Location Register) for big Telco carriers, many critical applications for manufacturing and retail businesses and a lot of others are deployed on HP NonStop servers today. These NonStop users do have processes in place informing their operational staff about any system alerts. But alerts, reflecting critical business

situations, are normally not covered yet in such a scenario.

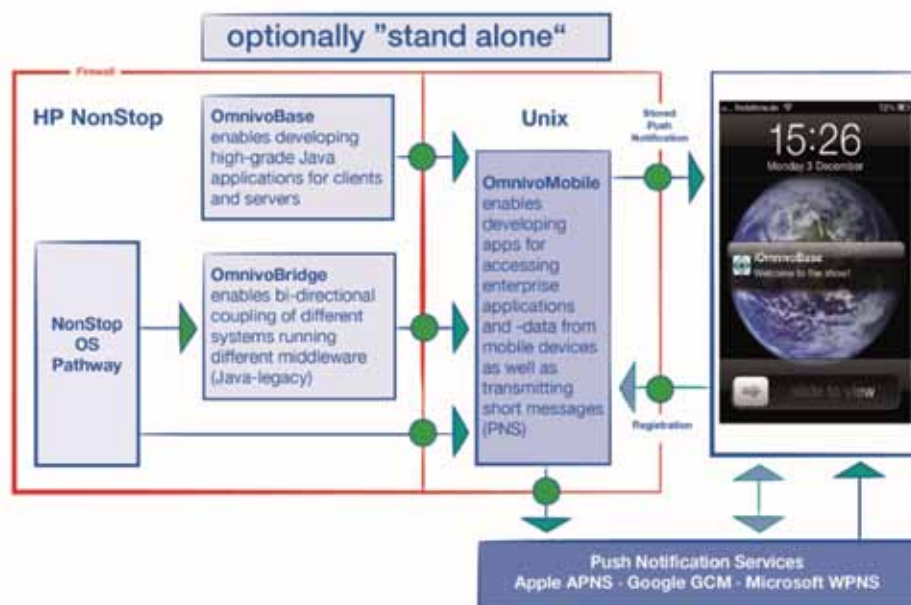
This could be a good start for providing instant information to management people about severe changes within business processes. The same mobile devices can consecutively be used to retrieve information about alert causes and to drill down other related information. Mobile devices, in this respect, are and will be devices with the highest user acceptance amongst these clients: you won't be able to get a high level manager carrying around an "always on" laptop. But he or she will accept one mobile device for all IT tasks.

Today's workplaces are becoming more and more a sort of "everywhere". Rapidly increasing numbers of enterprise users are already utilizing communication- and collaboration tools on Smartphones and Tablets. Managers within enterprises want to retrieve information almost everywhere and at any time for making the right decisions instantly. But also enterprise areas, not yet covered by the enterprise IT, like for example external stores, can easily and cost effectively be integrated with current IT infrastructures. Data from production applications can be turned into everywhere available information immediately.

### OmnivoMobile

Following these actual market trends, CommitWork had decided to provide its new product OmnivoMobile (first release is already available), allowing mobile devices to be easily integrated with HP NonStop based applications.

OmnivoMobile is doing the next step for NonStop users by enabling development of native applications (apps) on mobile devices for accessing enterprise applications and – data. Only such native apps permit utilizing mobile device components like video camera, GPS receiver and allow programmatic interactions with other installed apps like calendar, contacts and e-mail. Working just with Browser based applications on mobile devices, is not enabling access to those device components and therefore restricting utilization of most mobile device features.



Pic. 2: OmnivoMobile architecture

Other examples for perfect usages of mobile devices within enterprises could be image capturing, scanner replacement and utilizing GPS data for tracking systems. As a very specific feature, OmnivoMobile allows Push Notification Services (PNS) for the most important mobile OS (Operating System) providers. Using PNS, text messages and all kinds of other information can be transmitted and processed, like for example part numbers. OmnivoMobile allows communication with existing NonStop legacy applications utilizing OmnivoBridge as well as all enhanced features of CommitWork's OmnivoBase. (Pic. 2)

Security and control of enterprise IT infrastructures are major issues, if privately owned Smartphones and Tablets are used. OmnivoMobile controls all devices and apps as well as messages and message types and stores such data long term. It provides highest levels of security for all transactions by utilizing secure access via HTTPBasicAuthentication and encodes transmitted messages additionally. OmnivoMobile can utilize enterprise internal WLANs, mobile devices, entering Intranets from external networks, access thru HTTPS or VPN tunneling. Because of OmnivoMobile's architecture, there is no need to access NonStop servers directly from the Internet. Additionally implemented features like "Denial of Service Blocker" and "Service Filter" are completing OmnivoMobile's security concept.

### OmnivoMobile's features at a glance

- OmnivoMobile allows sending just one PNS message (Push Notification Service) to different mobile devices coming from different vendors, based on iOS, Android or Win 8.
- Delivery of PNS messages is normally not guaranteed. OmnivoMobile stores previously sent PNS messages, allowing mobile devices to explicitly recall these messages. Thru this mechanism delivery of PNS messages can be guaranteed. It controls all devices and apps centrally as well as messages and message types and stores such data long term. Additionally, an expiration date can be specified for PNS messages.

- Certain mobile devices can be grouped. A PNS message can be sent to a specified group of mobile devices. The group "all" exists by default. Registering new mobile devices adds such devices to the group "all".
- OmnivoMobile allows disabling certain mobile devices or groups of mobile devices or certain programs or certain vendor PNS temporarily. After re-enabling, OmnivoMobile will decide, whether a PNS message is obsolete or it is still to be sent.
- OmnivoMobile can utilize enterprise internal WLANs, mobile devices entering Intranets from external networks access thru HTTPS or VPN tunneling.
- OmnivoMobile provides highest levels of security for all transactions by utilizing secure access via HTTPBasicAuthentication and encodes transmitted messages additionally. Other features, implemented for completing OmnivoMobile's security concept, are "Denial of Service Blocker" and "Service Filter".
- OmnivoMobile's architecture prevents from accessing NonStop servers directly from the Internet.
- For developing apps on mobile devices, a specific library and programming hints are provided. Especially Android based mobile devices do not support badges, but OmnivoMobile provides such a feature. Additionally, OmnivoMobile allows playing sounds at arrival of PNS messages.

### Sources:

[www.forbes.com/sites/sap/2012/08/31/top-50-ipad-rollouts-by-enterprises-schools/](http://www.forbes.com/sites/sap/2012/08/31/top-50-ipad-rollouts-by-enterprises-schools/)

[www.gartner.com/DisplayDocument?doc\\_cd=211735&ref=g\\_noreg](http://www.gartner.com/DisplayDocument?doc_cd=211735&ref=g_noreg)

[www.idgconnect.com/download/8007/ipad-business-survey-2012?source=connect](http://www.idgconnect.com/download/8007/ipad-business-survey-2012?source=connect)

## NonStop Nuggets

Have you tried the new database management tool MXDM available as of NonStop SQL 3.2? For those of you who like the command line interfaces, you can invoke `rmxci` from MXDM.