

Shell EP

EP-GI-NG

**Application Compatibility and
Packaging team**

**GI-NG Basic environmental information
for Third Party Vendors**

**Version 2.0
01 February 2007**

Version Control

Scope

The purpose of the document is to provide vendors and their developers some basic information on the next Shell desktop. Incremental updates to the document will be published on the Shell internal network.

Target Audience

All who are involved in creating applications and making these available in the GI-NG Shell environment.

Owner/Author

Chris Zaal

Version History

Version Number	Revision Date (dd/mm/yyyy)	Contributor's Name	Revision Description
0.1	30-08-2006	Chris Zaal	Initial version based on GI 1.x document
0.2	29-01-2007	Chris Zaal	Updated .Net policies config
0.3	01-02-2007	Chris Zaal	Review from Kok Chee added

Approval Signatures

Name	Title
Maureen Nanang	EP GI NG Application Compatibility and Packaging Project Manager

Microsoft, Windows, and Windows 2000 are registered trademarks of Microsoft Corporation. All other products or services mentioned in this document are covered by the trademarks, service marks, or product names as designated by the companies who market those products.

Contents

1	WINDOWS VISTA, BASIS FOR GI/NG, A LOCKED ENVIRONMENT BY DEFAULT	4
2	THE GI-NEXT GENERATION DESKTOP	5
3	MICROSOFT .NET FRAMWORK 2.0 SECURITY POLICIES.....	6

1 Windows Vista, basis for GI/NG, a locked environment by default

The Shell Group Infrastructure Desktop, GI-D, will be based on Windows Vista Enterprise Edition. The current position is to provide the Technical Computing community, who explicitly need to address more than 2Gb data in their memory space for their applications and models, the Vista 64-bit model.

However, the common GI-D 2 machine will be considered to run the 32-bit version, which runs by default in locked down mode. This means that the GI-D users have no administrative privileges, which was the default install option with Windows 2000 and XP.

The advantage of running in a locked environment is that the system is significant less vulnerable to viruses, spy- and other mal-ware, and that the system is more stable to the enterprise environment.

Using Windows Vista means that the users are unable to perform task below, without a User Account Control message box popping up, which is default Windows Vista behaviour. The standard user in Shell will be unable to do any of the tasks below¹:

- The Windows Vista user will not be able to install software from CD or Internet, or uninstall pre-installed software.
- The Windows Vista user has no privileges to create directories or add/delete/modify files in the root of the C:\ drive
- The Windows Vista user has no privileges to create directories or add/delete/modify files in C:\Windows and subdirectories.
- The Windows Vista user has no privileges to create directories or add/delete/modify files in C:\Program Files and subdirectories
- The Windows Vista user has no privileges to edit the registry or write entries in HKLM, HKCR and HKU.
- The Windows Vista user has a roaming profile and has modify rights in the Users Folder that originally resides under C:\Users\%UserName%\ but in GI-D is redirected to the network.
- The GI-D user will be able to install software via the Advanced SMS Client interface or Add/Remove Software. There he will find all software he is allowed to install.
- Software distribution is managed through Microsoft System Centre & Configuration Management (SCCM).
- Applications are installed via Windows Installer and therefore based on the MSI format.
- Applications that are not shipped in msi format will be packaged in Kuala Lumpur to allow Shell to distribute it to the desktop.
- Temporary application data need to be stored in C:\Users\%UserName%\Local\AppData\Application Name
- Application User preferences need to be stored in HKCU if it concerns registry settings or C:\Users\%UserName%\AppData\Roaming\Application Name when the settings need to roam with the profile and can not be stored in the registry.

¹ Shell is in the process of engineering the platform, which could impact the security settings.

2 The GI-Next Generation desktop

The GI-NG desktop is based on²:

- Windows Vista Enterprise Edition both 32-bit and 64-bit versions.
- Internet Explorer 7
- Windows DAC version 6.0 (MDAC 2.8 SP1 on XP)
- Windows Installer 4.0
- MS Office 2007 Standard with multi language packs
- MS SQL Express 2005 SP1
- .Net Framework 2.0
- Oracle 10g Client
- Java Runtime Environment 1.6
- SAP GUI 7.1
- Anti virus software
- Acrobat reader 7
- Winzip 10
- MS SMS Advanced Client

Applications that need to run within Shell should be able to work with the OS, middleware and applications mentioned above. The list above is meant as minimal guideline and should be treated with discretion and not be disclosed to other parties.

² Software versions can change. Please verify with the AppCompat team the latest software versions.

3 Microsoft .NET Framwork 2.0 Security Policies

Within Shell it is not possible to open up the Machine runtime security policy beyond the Microsoft default settings. This policy level file is located at:

C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\security.config. Only modification to this file to narrow down on the default policy will have effect in the GI-D environment.

Shell added a general Code Group in the Enterprise Runtime security policy, called My_Computer_Zone group, that will run with Full Trust which is the Microsoft default. Specified as follows:

Assemblies matching the membership condition are granted this permission set at the current policy level: FullTrust.

This policy level file is located at:

C:\Windows\Microsoft.NET\Framework\v2.0.50727\config\enterprisesec.config.