

Pmi
Performance Management Intelligence

Technology & Security

– makes your department heads think like a CFO

Released October 2010

Table of Contents

Introduction.....	3
Server Hardware	3
Property Software	3
User Software	3
Other Requirements	3
PMI Upload Agent.....	4
Accessing the PMI Application	4
Securing the communication.....	4
Environment Overview	6
Fig. I – Dataflow	6
Fig. II – PMI Hardware Infrastructure	6
Fig. III – PMI Information FLOW	7
Fig. IV – Communication Overview	7

Introduction

PMI is a solution developed with and on Microsoft.Net technology running on Microsoft Internet Information Server 6 and Microsoft SQL Server 2005. The PMI application is hosted on a central server(s), and available for the users through their local installed Microsoft Internet Explorer.

Data from the customers' source systems are transferred to the PMI server(s) with our application PMI Upload Agent.

Server Hardware

The server environment (Verizon Business Server Center, Oslo) is based on VMWare 3.5u4 running on 5 servers with the following configuration:

- Dell PE R710 with 8x Intel Exeon 5570 3,0 Ghz with 72 GB RAM.
- 8x Gbit NIC against SAN and Internet.

There are 5 main virtual VMWare servers:

- 2 Web server
- 2 Database servers (64 bits)
- 1 Batch server (handling data import)
- In addition, there are servers for AD, DNS and Backup.

Property Software

- PMI Upload Agent (see chapter PMI Upload Agent)

User Software

- Microsoft Internet Explorer 6.x or higher
- Microsoft Excel 2003 or higher

Other Requirements

- d2o support team needs administrator access to the servers
- Depending on the source systems, there needs to be a nightly procedure for automatic/manual export to file/xml/webservice. In most cases also an ODBC connection from the PMI server to Time systems.

PMI Upload Agent

For upload of source files to PMI, d2o has developed a web service, "pmiUploadServer" (PMIUS), that is accessible via wsvpmi.d2o.biz. It will use https (Hypertext Transfer Protocol Secure) for transferring the files.

For this purpose the PMIUS works together with the "PMI Upload Agent" (Agent) that is installed on a Workstation or Server (interface pc) at the customer's side. The Agent has access to the customer's local PMS and POS source files and can transfer data over Internet (via port 80; no Firewall adjustments needed) to the PMIUS.

On the interface pc the Agent is installed in a folder on a local (unmapped) drive (standard `c:\d2oAgent`). The application runs as a system tray application under the current logged on user. This user needs to have full read and write permissions to that folder.

It consists of the following files:

- `PmiUploadAgent.exe`: The core Agent application.
- `Interop.Shell32.dll`: Used to add a shortcut to the desktop and start-up folder (default desktop is off, auto start-up is on).
- `pmiUploadAgent.config`: Configuration file that has a unique hotel id per hotel that it serves. This id identifies the hotel to the web service and directs where the files are placed on the server.
- `pmiUploadAgent.status.xml`: Status registration file. This file contains the status of sending the files between sessions and can also be used to get actual information on the sending of the files. At startup and when changes happen the client and the server status are synchronized on contact with the server.

Accessing the PMI Application

The communication between the customer's local browser (Internet Explorer) and the PMI server is using HTTPS (Hypertext Transfer Protocol Secure; SSL).

Securing the communication

For both file transfer and application use d2o can in addition to https offer several alternatives regarding securing the communication between the customer's local client/network and the PMI server:

Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a data stream. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session.

IPsec can be used to protect data flows between a pair of hosts (e.g. computer users or servers), between a pair of security gateways (e.g. routers or firewalls), or between a security gateway and a host.

Secure Sockets Layer virtual private network (SSL VPN) OpenVPN is a full-featured open source SSL VPN solution that accommodates a wide range of configurations, including remote access, site-to-site VPNs, Wi-Fi security, and enterprise-scale remote access solutions with load balancing, failover, and fine-grained access controls. OpenVPN's lightweight design sheds many of the complexities that characterize other VPN implementations.

The OpenVPN security model is based on SSL, the industry standard for secure communications via the internet. OpenVPN implements OSI layer 2 or 3 secure network extension using the SSL/TLS protocol, supports flexible client authentication methods based on certificates, smart cards, and/or 2-factor authentication, and allows user or group-specific access control policies using firewall rules applied to the VPN virtual interface. OpenVPN is not a web application proxy and does not operate through a web browser.

Both for IPsec and SSL VPN, the communication is set up and configured in cooperation with the customer and their security standards. d2o is of course also open for discussing other alternatives for securing the communication.

Environment Overview

Fig. I – Dataflow

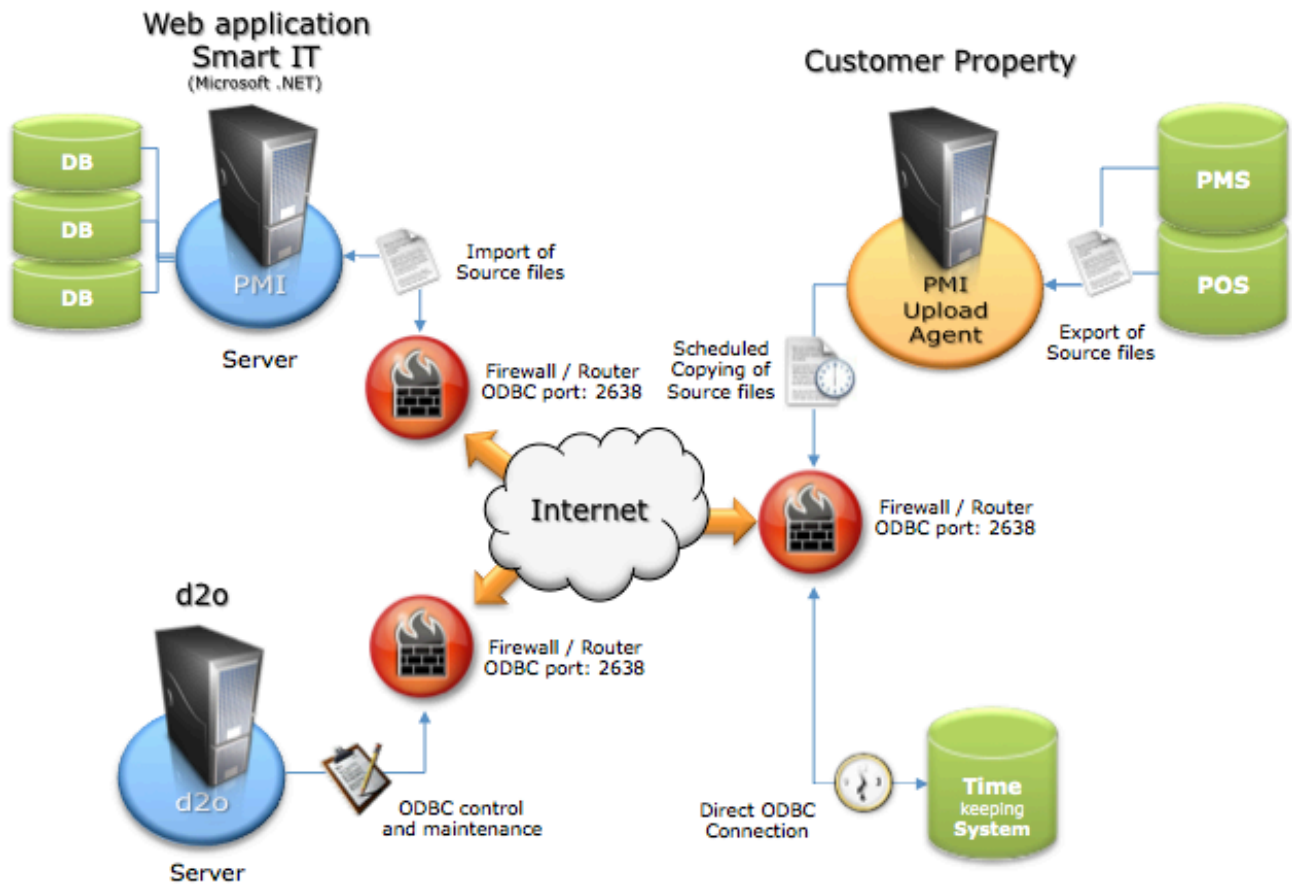


Fig. II – PMI Hardware Infrastructure

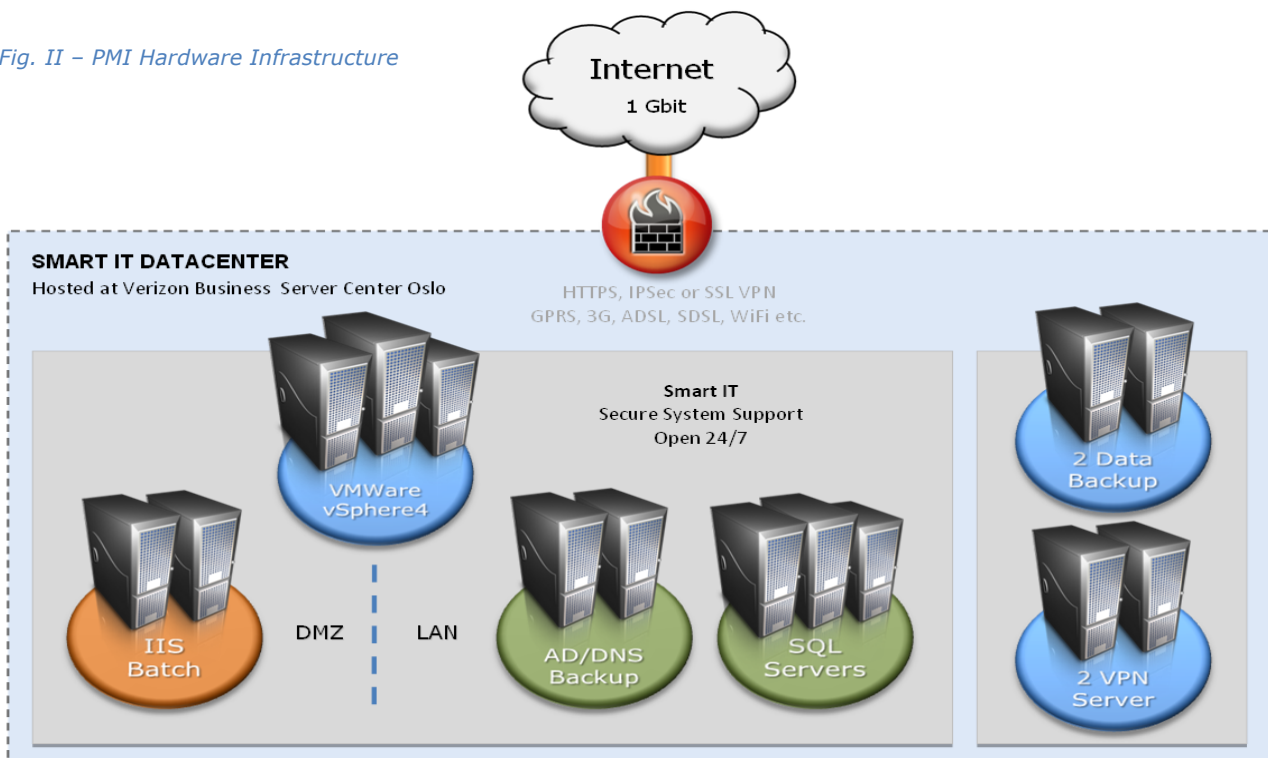


Fig. III – PMI Information Flow

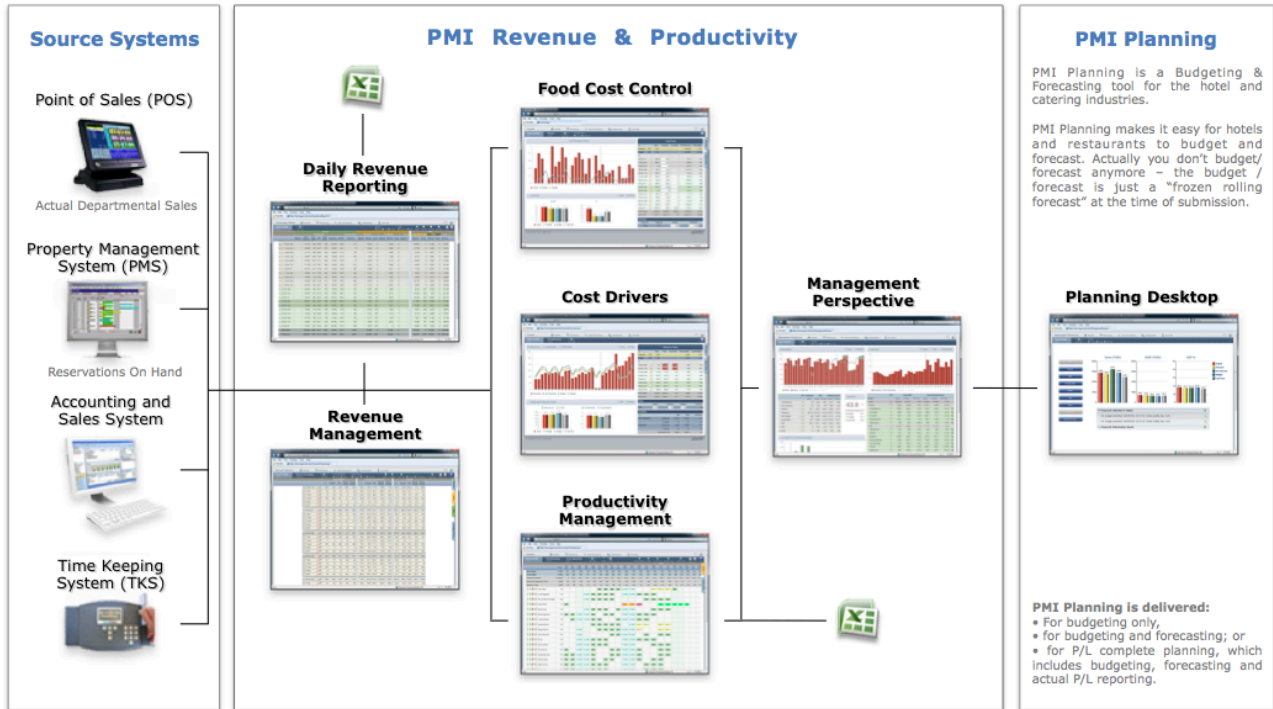


Fig. IV – Communication Overview

