CGMS-XXXIII JMA-WP-16
Prepared by JMA
Agenda Item: IV/1.1
Discussed in WG IV

Outline of the WMO Information System (WIS) VPN Pilot Project in Regions II and V

This working paper reports on outline and status of the WMO Information System (WIS) VPN Pilot Project in Regions II and V.

Outline of the WMO Information System (WIS) VPN Pilot Project in Regions II and V

1 Introduction

The Future WMO Information System (FWIS) is a single coordinated global infrastructure that is intended to serve all relevant WMO programmes. It would facilitate international exchange of meteorological and hydrological data.

The Fourteenth WMO World Meteorological Congress (May, 2003) emphasised that the implementation of FWIS should build upon the most successful components of the existing WMO information systems in an evolutionary process, through a smooth and coordinated transition. The FWIS was renamed to the WMO Information System (WIS) at the 57th Session of the Executive Council (June 2005).

WIS consists of diverse types of communication links as available, appropriate and cost effective, including dedicated links and networks, satellite-based systems and the Internet. In particular, communication component of the WIS would build upon the WMO Global Telecommunication System (GTS) with respect to the requirements for highly reliable delivery of time-critical data and products, and the Improved MTN GTS would be the basis for the core communication network. The Congress also noted that the further development and implementation of WIS would be pursued through relevant pilot projects.

Triggered by the Implementation Coordination Meeting on the GTS and the Information Systems and Services (ISS) in Region V (Wellington, December 2003), the FWIS Virtual Private Network Pilot Project (VPN-PP) has started, collaborating with GTS Centres and National Meteorological Centres in Regions II and V on a voluntary basis, aiming at evaluating the feasibility of Internet-VPN and related technologies to be applied to WIS as a means of communication. The purpose of the project is to contribute to WIS development through a feasibility study of the WIS concepts.

2 WIS VPN Pilot Project in Regions II and V

Although the Internet is possibly an important and preferable means of communication especially for small Centres to be benefited from the WIS, there arise some concerns of not only connectivity, but also throughput and security when using the Internet operationally. In the forthcoming WIS environment, broadband circuit will be indispensable for National Centres (NC) to fully enjoy access to satellite imagery data and/or numerical products from the Global Information System Centres (GISC) and/or the Data Collection or Product Centres (DCPC). As for the Internet security, investment for a countermeasure against threats and its cost-effectiveness could be the major consideration. The use of the Virtual Private Network (VPN) technology is one of the promising solutions to evade annoying security issues. VPN by the IP Security Protocol (IPsec) is becoming popular nowadays on account of its convenience.

The purpose of the VPN-PP is to find out and evaluate the practical use of Internet

VPN under various conditions such as different levels of IT expertise, different levels of access to the Internet in cooperation with NMHS centres.

In 2004, preliminary basic studies and technical tests of the data transport level were conducted and the result was reported to WMO WIS related meetings. Furthermore, an advanced phase is currently being in progress with the wider target of application level.

2.1 Initial phase (2004)

(1) Outline

In support of the collaborative project among two Regions, eleven WMO Members - Australia, Brunei, China, Hong Kong, India, Japan, Republic of Korea, Malaysia, New Zealand, Saudi Arabia, Vietnam - participated in the VPN-PP on a voluntary basis. The scope and location of the VPN-PP in the WIS communication structure is illustrated in Figure 1.

(2) Evaluation items

Baselines for evaluation were as follows:

a) Empirical feasibility to use the Internet VPN for:
- branch links between a GISC, DCPCs and NCs on a routine basis
- ad hoc request/reply between a portal site for data request and each requesting centre or each data source centre
- backup and/or complement links of a core network among GISCs

b) Practical views on VPN implementation
- Geographical features
- Extraction of difficulties
- Cost consideration
- Impact evaluation of technical gaps between centres
- Future prospect

(3) Outcome

(i) Use of the Internet VPN

It was a common recognition among engineers at the beginning of the Project that Internet VPN by IPsec is manufacturer dependent and difficult to configure in a heterogeneous environment such as WIS. As a result of the Project, Internet VPN based on IPsec technology turned out to function well; all Centers except one were able to establish a VPN connection in spite of various platform and unknown vendor configurations. The project revealed that the connectivity depended on the selection of a common parameter set for VPN equipment, which could be accepted by both ends. A reasonable amount of different sets of IPsec parameters and IKE types were tested with great success. Also it was confirmed that data were smoothly exchanged without any unexpected tunnel teardowns and re-negotiations after expiration of the IPsec timers. Although VPN overhead definitely exists especially in high throughput cases, it seemed

not always be critical.

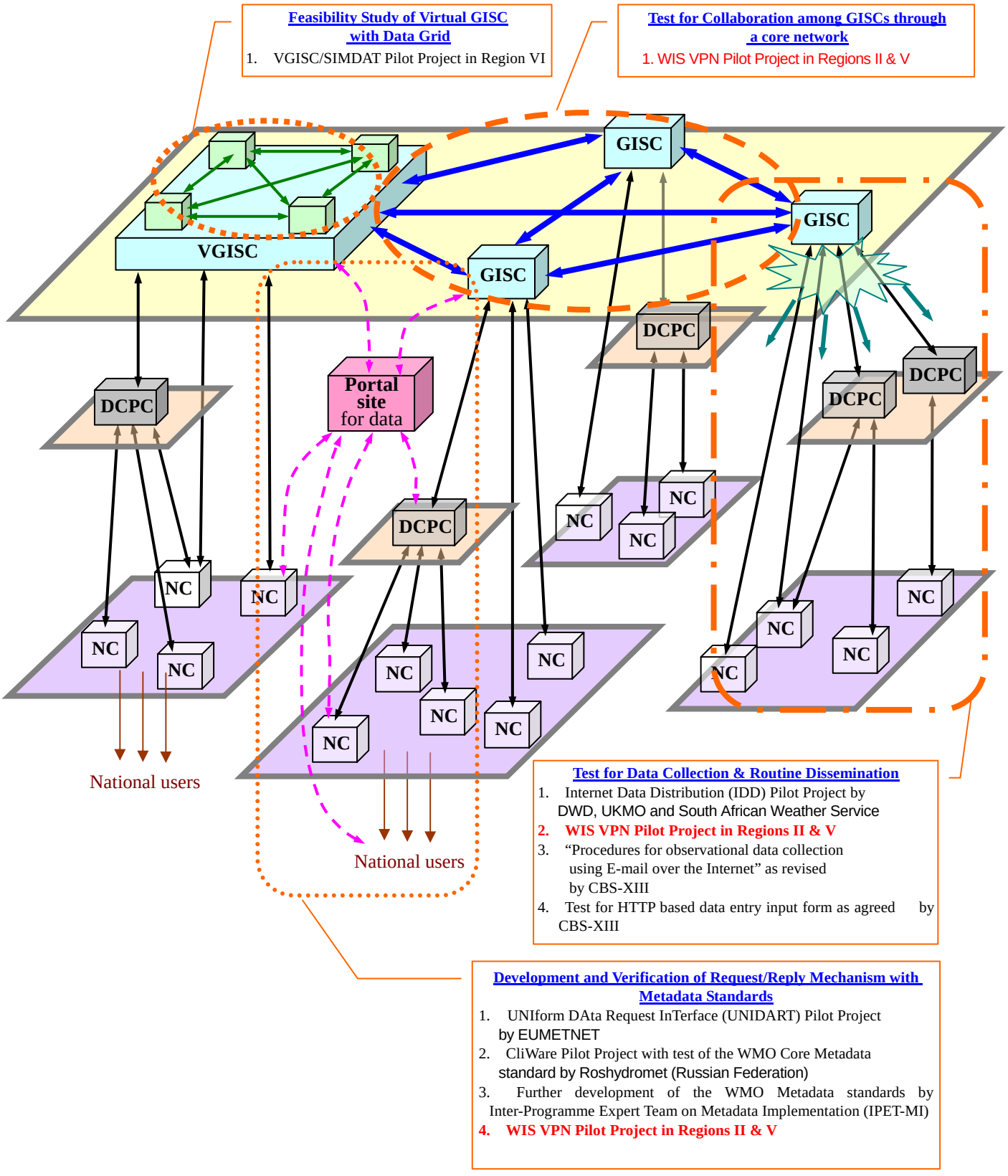

Figure 1: Scope and location of pilot projects in WIS communication structure

(ii) Required performance in GISCs

It is presumed that a GISC will have many branch links with NCs and DCPCs. If most of them are VPN, the concentration impact to the GISC will not be negligible. The GISC may need to install and maintain one of the highest-performance VPN products which are implicitly very expensive even if performance of products in market is improved year by year. It may be a burden to the GISC in cost and human resources to maintain their performance to meet the requirements.

(iii) Technical assistance and remote maintenance

Although IT innovation has been improving worldwide availability of network technology, there are still technical gaps in practical aspects between WMO Members. If a GISC can be a technical sponsor who assists the Centres in its area of responsibility, it will be very easy to get an operation network up and running within a reasonable timeframe.

In this project, some sites were more familiar with the technology than others. For example, Melbourne (Simulating GISC) provided assistance that was needed by other Centres using “remote maintenance” effectively.

2.2 Advanced phase (2005 - 2006)

Taking over the initial phase, the advanced phase started in 2005 including two additional Members, Iran and Oman, aiming at further study and evaluation of Internet-VPN technology and its application.

It is required that the pilot project be expanded to the WIS application level in cooperation with other pilot projects for WIS application components such as request/reply, portal and metadata standards. In this context, a draft plan for next two years is under development from the following viewpoints:

- Possible cooperation with UNIDART and VGISC projects in the Region VI
- Comprehensive tests from transport level to application level
- Simulation of NC operation with prototype applications, e.g. SATAID, supported by Pandora data server
- Data management such as WMO metadata standard and code migration
- Study of authorization and authentication methods for secure data reporting and providing including mobile environment
- Expanding the number of participants in the Regions

The advanced phase will consist of a few thematic sub-phases. Figure 2 shows examples of conceptual images in the sub-phases.

To facilitate the progress of the project, JMA established a web server so that

participants could share current status and progress. The server provides various information and functions related to the project, e.g. recent proceedings, project documents, a list of participating centres, discussion function among Members, and real-time status of the VPN links. Prototype applications for the project, such as SATAID, are also provided and could be downloaded from the server.

3 Conclusion

The initial phase of the VPN Pilot Project ended with great success. The Project proved the feasibility of Internet-VPN; Internet-VPN is adaptable to small Centres which had insufficient expertise and needed technical assistance; and those small Centres could share the benefit of WIS. The outcome was reported to the WMO WIS related meetings and was appreciated. Following the initial phase, advanced phase started.

The latest status of the project will be reported during the CGMS-XXXIII meeting.

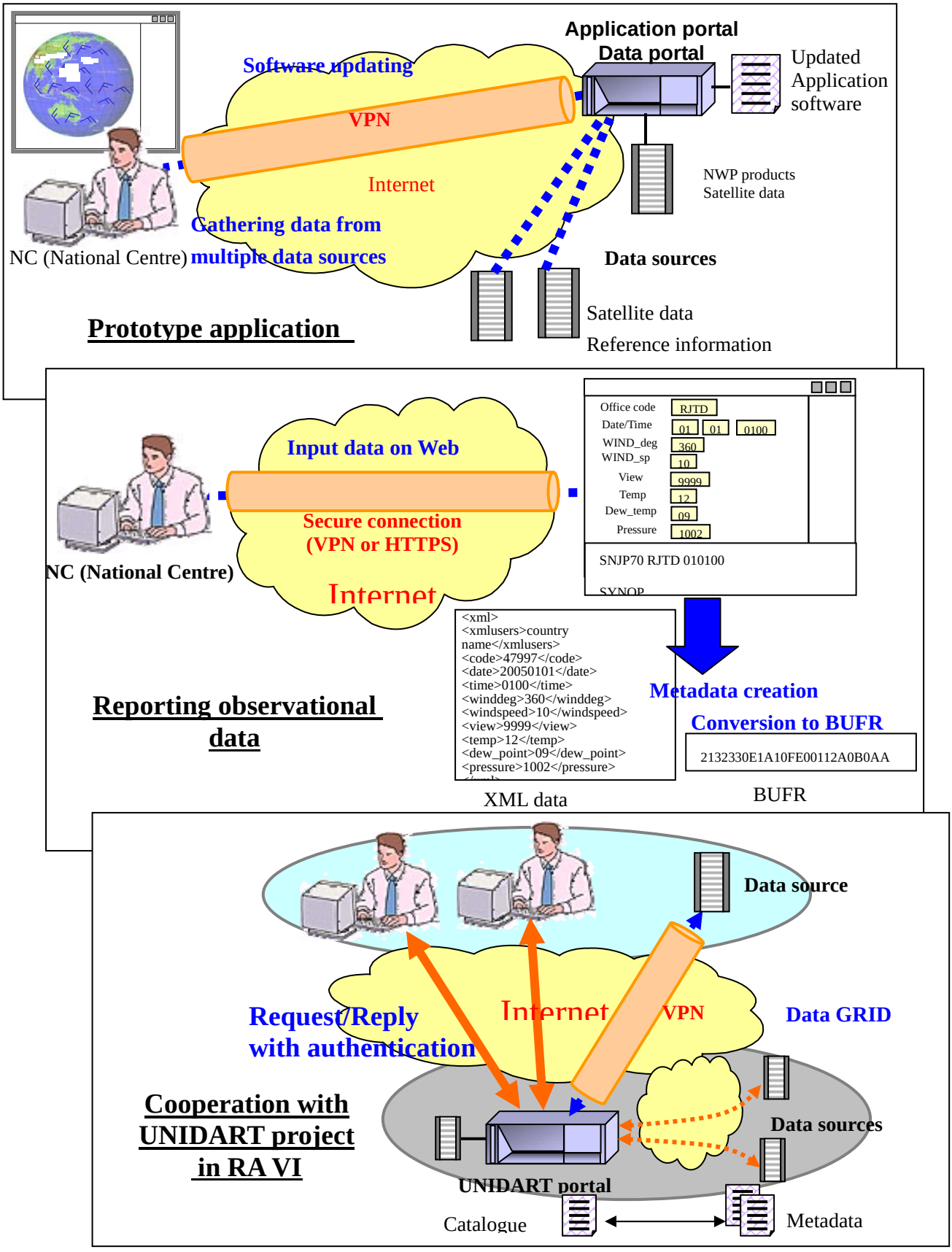

Figure 2: Examples of thematic sub-phases in the WIS VPN Pilot Project advanced phase