

## SECURE MILITARY MESSAGING IN COALITION OPERATIONS

Neville F. Parker<sup>1</sup>, Marie Henderson and Charles R. Moore

**Abstract.** Military operations are increasingly being conducted by ad hoc coalitions. The need to provide a communications and information system (CIS) infrastructure for coalition members with connections to the command support systems of contingent members, particularly that of the lead nation, poses difficult information security issues. This paper discusses the heightened need to support need-to-know separation within a coalition environment compared with a single nation tactical deployment. Security architecture options for a coalition CIS are discussed and the enhancement of these architectures with Public Key Infrastructure (PKI) per-message confidentiality services is proposed. The integration of PKI technology within a coalition deployment is explored, as is the extension of the confidentiality services offered by this technology to agencies external to the coalition deployment via public and rear-link networks.

### INTRODUCTION

International military operations are increasingly being conducted as coalitions, such as in the Gulf War, Bosnia, and Timor. While some nations such as those in NATO have considerable experience of combined operations, it is increasingly probable that coalition forces will be composed of diverse nations without any history of combined operations. These coalitions will exhibit many or all of the following characteristics:

- **Large number of contingent members.** Coalitions may contain a large number of contingent nations, perhaps 20 or more. These members may have significantly different motivations for their presence in the coalition, reflecting their respective national strategic priorities.
- **Single lead nation.** An authority, such as the UN, will designate a nation as the lead nation to provide the coalition commander.
- **Differing levels of trust.** Diversity among national contingents may result in differing levels of trust between contingent nations.
- **No coalition infrastructure.** A coalition operation may occur in a region where there are no fixed military communication assets. Coalition members may have non-interoperable equipment and different processes and procedures.
- **Provision of communications infrastructure by Lead Nation.** The lead nation would typically provide the communications and information systems (CIS) infrastructure, although other nations may provide some CIS components.
- **Common CIS system.** A common command support system and communications system is likely to be used in the coalition headquarters, accessed by liaison officers from different contingent members.
- **Deployment evolution.** The deployment may change over time, with respect to contingent members, command arrangements and involvement of civil agencies.

Although the need to share information for command and control (C2) support is essential, it is unlikely that within a

large coalition all contingent nations would be prepared to share information equally. However, within the coalition there may be sub-groups of nations where high levels of information sharing might occur. The dilemma for contingent nations is their need to protect their national systems while supporting a degree of integration with the coalition system. For the Lead Nation this is particularly critical.

Current practice would create both a Secret Coalition and a Restricted Coalition network to mirror national systems. The classifications would be defined in coalition terms, instead of national terms, and the protection of these systems would reflect that of the respective national system. This paper explores the enhancement of a Restricted Coalition system with strong need-to-know protection for C2. The classification level of coalition C2 systems is discussed further in the final section.

Within a traditional national Restricted Defence security infrastructure the requirement to segregate need-to-know information is not particularly high, except for very specific types of information, and is not typically enforced by any technical security means. Within a coalition system the requirement for need-to-know separation is assumed to be high and technical enforcement of separation may be advantageous. Secure messaging products utilising Public Key Infrastructure (PKI) technology (often called 'Certificate Management Infrastructure' (CMI) in the military literature) is now being adopted in commercial and military environments and provides such a technical capability. NATO and AUSCANNZUKUS nations are beginning to deploy PKIs to provide such capabilities.

Fundamental to the solution of these security problems is the need for a security architecture, loosely defined as a series of elements and associated functions to enforce or implement security policies. Associated with security functions are security mechanisms, ranging in strength from those capable of separating information of different security classifications to those with only sufficient strength to separate need-to-know information within a single security classification level. Some mechanisms operate at a coarse level of access control granularity while others implement fine-level granularity. The remainder of this paper explores the possible integration of PKI technology into the security architectures required by coalition operations and the potential capability enhancement this technology offers.

<sup>1</sup> Systems Engineering Manager, Directorate of Command and Intelligence Support Systems, Defence Materiel Organisation, R3-3-090, Russell Offices, CANBERRA, 2600, AUSTRALIA.