# Protected Core Networking: An Architectural Approach to Secure and Flexible Communications

*Geir Hallingstad and Sander Oudkerk, NATO C3 Agency*

## ABSTRACT

Protected core networking (PCN) is a concept intended to be used to implement a flexible transport infrastructure that supports future military operations based on network enabled capability (NEC). PCN is based on creating a loose coupling between information domains and the transport infrastructure, and focusing on the provision of high service availability, also in high-threat environments. This architectural approach highlights a number of emerging and novel concepts where research and development is needed to properly support NEC.

## INTRODUCTION

Network enabled capability (NEC), a concept similar to network centric warfare, is a new way of performing military operations that is appropriate to the current and future operational environments. The requirements for technology support are large, mainly focused on providing solutions for effective sharing of information and flexible, widely available communications, the first depending on the latter.

The objective of this article is to explain protected core networking (PCN), an approach to creating a secure and flexible network and communications infrastructure that supports the NEC environment. PCN combines a number of current and cutting edge principles and techniques with some novel concepts, aiming to create a transport network[1] that fulfils the NEC requirements.

The work presented in this article is the result of a research program recently started at the NATO C3 Agency.[2] It should be noted that PCN is a concept in development, and further research and prototyping is necessary in order to reach a fully functioning network based on PCN. In this article the main PCN components and interfaces are described at a high level. While some of the concepts and techniques necessary for PCN are available and well known, many are either immature or novel. The intention of the authors is to show that the PCN approach can fulfill the needs of an NEC environment, but more research is required in the field of network and communication systems.

The first section of this article reviews the network and communications requirements NEC imposes. The following section explains the concept of PCN, while the next two sections explain in more detail how a system based on PCN works. We then give the definition of PCN terms and interfaces. Next, we compare PCN to other approaches and outline research challenges, and the final section concludes the article.

## SUPPORTING NETWORK ENABLED CAPABILITY

Network enabled capability is an approach to military operations in response to a changing environment. Today's operations have effects in several dimensions (e.g., social and economic in addition to military). In addition, multiple entities, including military, government, and international organizations, are present. The bottom line is that in such a complex endeavor [1], it is impossible to accurately predict the outcome of operations, and the ability to adapt quickly to a given situation becomes key to success.

To adapt quickly, a property also referred to as *agility*, it is necessary to perform decision making at the lowest levels of command, an approach called an *edge organization* [2]. To fully reap the benefits of the distributed decision making, edge entities must share awareness of the current situation. Therefore, each entity must have any necessary information available in a timely manner and be able to synchronize actions with other relevant entities, be they military or not. This goes well beyond what traditional military communications and information systems (CISs) were designed to do, and a new architectural approach is necessary.

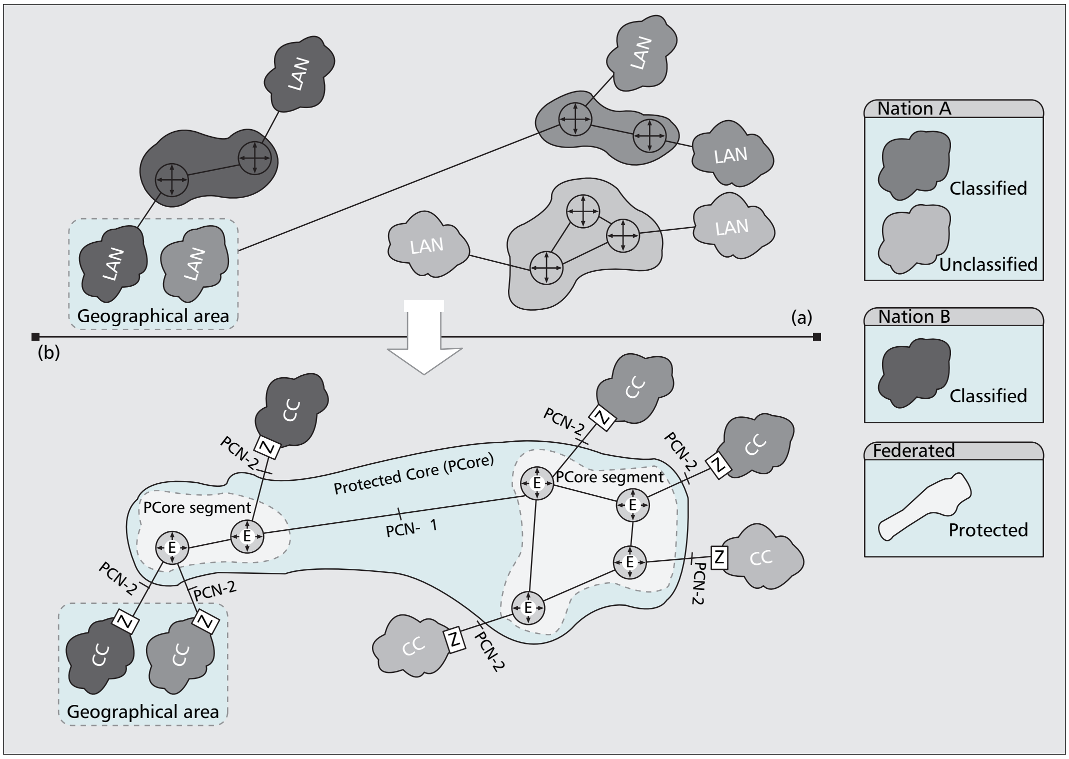
While individual improvements to current systems can help in supporting the transformation to NEC, a shift in the architectural approach is needed to fully enable NEC. By identifying an approach that accounts for the changed operating environment, the required research and technology can be identified, and progress toward NEC drastically improved. Without a coherent approach, chances are that conflicting approaches and technologies will stall or severely slow the

[1] *A transport network is a network that transports data between two parties.*

[2] *This work was funded under the NATO C3 Agency's Scientific Program of Work for NATO's Supreme Allied Command Transformation, Norfolk, Virginia.*

0163-6804/08/$25.00 © 2008 IEEE

PCN gives rise to a number of benefits for the users and the operators, as well as the system owners compared to current and emerging systems. However, to fully realize all benefits of PCN, further research is necessary



■ **Figure 1.** *Comparison of a) a traditional military network; b) a protected core.*

progress, meaning that military operations will have to be performed in the traditional way, even if the approach is becoming less effective.

## Protected Core Networking

PCN is a concept intended to be used for creating a transport network that supports the requirements of NEC operations. It uses an architectural approach that achieves both flexibility and security, an arduous task when not encompassed from the conception of the approach. The objective of PCN is not to define one specific system; rather, PCN will define the interoperability points that allow interoperability between heterogeneous systems that adhere to the PCN requirements. Therefore, this article does not describe a system, but describes the requirements to which a system must adhere.

PCN gives rise to a number of benefits for users and operators, as well as system owners compared to current and emerging systems, including support of dynamic environments and better cost efficiency due to the ability to share infrastructure. However, to fully realize all benefits of PCN, further research is necessary as there are areas where the required technology does not yet exist. The following sections explain the PCN approach, and a later section summarizes the research and development needed to progress.

### Designed for Flexibility

Consider the scenario shown in Fig. 1a, which shows a typical CIS situation in current military environments. The figure shows two nations and three networks, all at different classification levels. Two of the networks, one from each nation, are collocated geographically, each with its own communications link back to its native network.

The communications solutions for the networks in Fig. 1a are custom made based on the requirements for each individual system. An infrastructure tailored to a classified system usually cannot be used by any other system as this would break the information confidentiality, which is typically applied at the lowest layer in the communications stack (e.g., using link encryption). Similarly, a system tailored to a lower classification cannot be used by a higher classified system due to the absence of information confidentiality protection and the insecurity of the transport infrastructure from an availability perspective. In order to create a system that is both flexible and secure, it is necessary to separate the system into component parts that handle plaintext classified information and parts that transport information. This requires information confidentiality protection to be separated from the protection of the availability of the transport network.

In the PCN approach, shown in Fig. 1b, components that contribute to the transport of information are part of the protected core (PCore). The networks that handle classified information, referred to as colored clouds (CCs), are not part of the PCore. On the contrary, the CCs are the users of the PCore. CCs are responsible for ensuring information confidentiality of their respective information domains, and must therefore apply confidentiality protection measures before sending data to the destination CC through the PCore. This can be done by applying information confidentiality at a layer above the data link layer in the communications stack (e.g., at the network layer using IP network encryption).[3]

The CCs can use this approach to protect information confidentiality without loss of strength compared to the approach in Fig. 1a. However, it is the responsibility of the PCore to ensure that critical data is transported in a timely manner. The PCN approach is to create a trusted overlay network that controls service access and ensures service delivery to the CCs. A PCore does not handle plaintext classified information, and as such is not a classified network. However, the protection measures in a PCore are of similar strength but focus on protecting availability rather than confidentiality. This is the origin of the term *protected core*.

The interface between the PCore and the CCs is identified as service interoperability point (SIOP) PCN-2. PCN-2 is the point of service delivery from the PCore to the CCs. The internal implementation of a CC or PCore can vary, as long as both adhere to the PCN-2 specification. The PCN-2 interface creates a loose coupling between the CCs and the PCore that makes it possible to support mobility and clearly separates authority. Due to the separation of confidentiality protection and transport service availability, multiple colored domains can use the PCore, including those of other nations as shown in Fig. 1, given an agreed service level agreement (SLA).

The loose coupling will allow CCs to move to another location and reconnect to a PCore without any manual configuration. In this way no device or end user inside a CC will be affected by the move (logically). Seamless mobility is vital for entity agility; however, agility also depends on the size of the CCs, as an entire CC must be moved as one unit. A CC can vary in size from embedded systems to large networks supporting headquarters. Agility further depends on the physical extent of the PCore. Expanding the PCore by moving infrastructure components from a CC to the PCore would decrease the size of the CC and increase the extent of the PCore, both contributing to increased agility, at the cost of more IP encryption.

### SERVICES AT PCN-2

When supporting a wide variety of users, a number of different applications are foreseen to be supported (e.g., messaging, interactive voice, and videoconferencing). All these applications have different requirements for, say, bandwidth and latency. To support all necessary traffic classes, a PCore must provide quality of service [3, 4] support. This ensures that network convergence can progress, moving all services to a common network while maintaining service quality.

Furthermore, a PCore must provide transport services to networks and systems of different criticality; for example, an Internet connection for the purpose of welfare as opposed to a live transmission from an unmanned aerial vehicle or the transmission of friendly force tracking information. A PCore has to be able to provide multiple levels of precedence and pre-emption (MLPP) [5], so that critical traffic can take priority over traffic with lesser importance.

An effect of the architecture shown in Fig. 1 is that the protection of traffic flow confidentiality (TFC), previously provided by the classified infrastructure, must be provided by the PCore. Traffic flow refers to the information that can be observed by looking at the flow rather than the information within the payload of the packets. Traffic flow can often reveal that there is communications, the volume, and who is talking to whom. Traffic flow can be protected by, for example, using encryption at a low layer with padding of data such that the link is always fully utilized regardless of the actual traffic. In PCN TFC is a service offered by the PCore. Traffic that requires TFC traverses only links with TFC provision, as shown in Fig. 2.

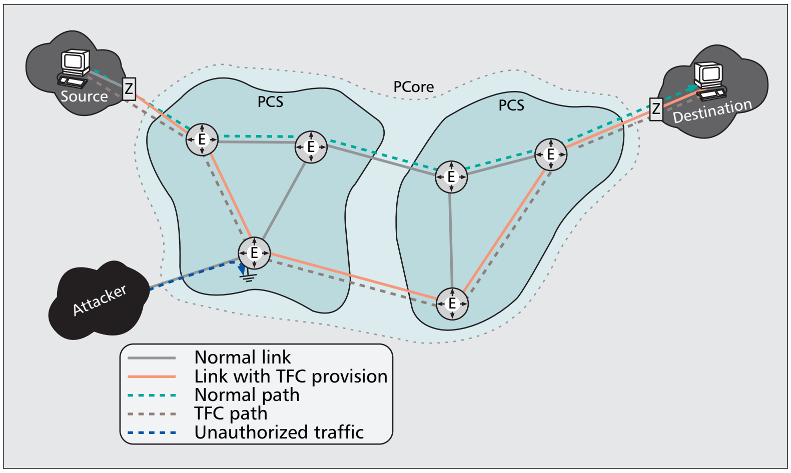


**Figure 2.** *A PCore routes traffic according to requirements and drops any unauthorized traffic.*

In order to ensure proper service, an SLA must be negotiated. This SLA must include discovering the services that are available and the usage parameters (e.g., bandwidth, delay, and priority). The SLA enables service predictability for the CCs, and gives the PCore the ability to differentiate services according to policy (e.g., ensuring that CCs with critical data are not prevented from receiving service).

### PROTECTION OF SERVICE AVAILABILITY

To be able to provide transport service to time-critical data, the PCore needs to take measures to ensure service availability. The PCore uses ubiquitous enforcement (E-) functionality that authenticates and performs access control on all connections, to both the users (CCs) and other components of the PCore itself. An attacker would not be able to flood the PCore, as the unauthorized traffic would be dropped at the PCore entry point, as shown in Fig. 2. Furthermore, the E-functionality must enforce the agreed SLAs, including rate and bandwidth consumption and priority marking.

In addition to pervasive security enforcement, the PCore must ensure robustness of service delivery. By capturing extended properties of each communications link and feeding them to a real-time risk assessment (RTARA), the operator should quickly realize when the network is subject to unacceptable risk, and can initiate mitigating measures.

The trusted overlay created by a PCore, and verified by a mutual authentication over PCN-2, makes richer interaction between classified domains and the PCore possible, e.g., with respect to QoS and MLPP. This way, CCs with time-critical systems can safely use the same PCore as

[3] *In the remainder of this article the term IP encryption will be used.*

*Third party links may have many different properties, both with respect to performance and security. One of the key aspects of PCN is to leverage the knowledge of the properties of third party links in order to assess the risk. The Es are the key components in reporting link properties and enforcing access control.*

other CCs, as long as the timeliness requirements are captured in the established SLA.

### A FEDERATED NETWORK

As a PCore can consist of multiple independent systems under sovereign national authority, no supreme authority exists. However, all participants have to coordinate efforts in order to achieve the common goal of sustaining a protected transport network, so the PCore must be federated.

A PCore is made up of one or more protected core segments (PCSs). A segment is under one authority and interconnects to other segments using interoperability point PCN-1. The implementation of the segments can differ, as long as the PCore requirements at PCN-1 are fulfilled. Interconnecting protected network segments is expected to be less difficult than interconnecting classified systems, as information confidentiality is not at stake. An implication of this is that nations can utilize each other's infrastructure, which could potentially lead to cost benefits.

## PROTECTED CORE SEGMENTS

A PCore can consist of one or more PCSs as shown in Figs. 1 and 2. The internal design of a PCS is by definition built on the principles of PCN. Even though the inner workings of a PCS are irrelevant to its users (the CCs), the fact that it is based on the principles of PCN has several benefits to the operators of the PCS.

### THE ENFORCEMENT OF A SECURITY POLICY THROUGHOUT THE PCS

The NEC operations that a PCS must support are highly dynamic and the management of the PCS has to respond accordingly in order to ensure that the network always supports the operation. The protection mechanisms have to consistently enforce a security policy that properly reflects the risk level of the network at any given time, ensuring proper service delivery. Ubiquitous policy enforcement requires coherent management.

Traditional ad hoc management does not provide the means to respond to changes in the network environment in an automated fashion; nor is it able to realize consistent enforcement of the policy due to separate management of security and network services. It also lacks the mechanisms to determine the status of the network with respect to the policy enforced.

In PCN the management agents that enforce the security policy are termed Es. The Es have to communicate with the PCS management system constantly in order to receive policy updates or report back their status with respect to the enforcement of the current security policy. In order to provide a trusted path through the PCS, a standard requirement in the PCS security policy is for each E to authenticate the link it monitors. As a result, all links in the PCS are authenticated.

One model that could meet the requirements for the PCS policy management is the model of policy-based management (PBM) [6, 7]. The Es then have the role of policy enforcement points. An alternative could be to use a Web services architecture [8] in which Es request the service of policy updates from the PCS management system, while providing the service of status updates to the PCS management system.

### USE OF THIRD PARTY LINKS AS TRANSPORT LINKS

PCN uses third-party links solely as transport links, overlaying a layer of trust. Traffic on a link is always checked to be authorized before being forwarded. Any link can be included, as long as the PCore access is properly protected, and the properties of the link are captured.

Third-party links may have many different properties, with respect to both performance and security. One of the key aspects of PCN is to leverage knowledge of the properties of third-party links in order to assess the risk. The Es are the key components in reporting link properties and enforcing access control.

### LINK PROPERTIES

Using link properties for risk assessment is not limited to third-party links but can be applied to every link in a PCS. A number of properties can be captured for this purpose, including not only communications characteristics such as bandwidth, latency, and error rate, but also security properties such as electromagnetic radiation, physical protection, and TFC.

Security properties of a link can be related to the traditional security objectives. Link confidentiality properties relate to how difficult it is to monitor the link, physical protection of the link, and link encryption. Link integrity relates to how difficult it is to modify, inject or corrupt traffic on the link. Link availability says something about the performance of the link, for example how easily the link can be attacked or how difficult is it to cut the cable or jam the frequencies used.

For every link the properties have to be captured by the Es and communicated to the management system. In the management system the link properties have to be recorded and analyzed (Fig. 3). The link properties can also be used to make routing decisions given a specific service request, for example TFC.

### REAL-TIME AUTOMATED RISK ASSESSMENT

The analysis of link properties is part of an overall RTARA that has several potential uses. First, it can help to identify weak points in the network, such as single points of failure, areas with low bandwidth or low-reliability coverage, or communication paths that can be established solely through unreliable third party links. Second, it can serve as input to the management of the PCS, and the security policy can be updated accordingly. Third, it can serve as the primary input to a dynamic accreditation system which assures the operator that the current system meets the applicable accreditation criteria at that point in time.

### DYNAMIC ACCREDITATION OF A PCS

Each PCS constitutes a security domain, which falls under the authority of a sovereign national security accreditation authority (SAA). A change to the PCS network infrastructure (e.g., the inclusion of a connecting CC) requires re-accred-

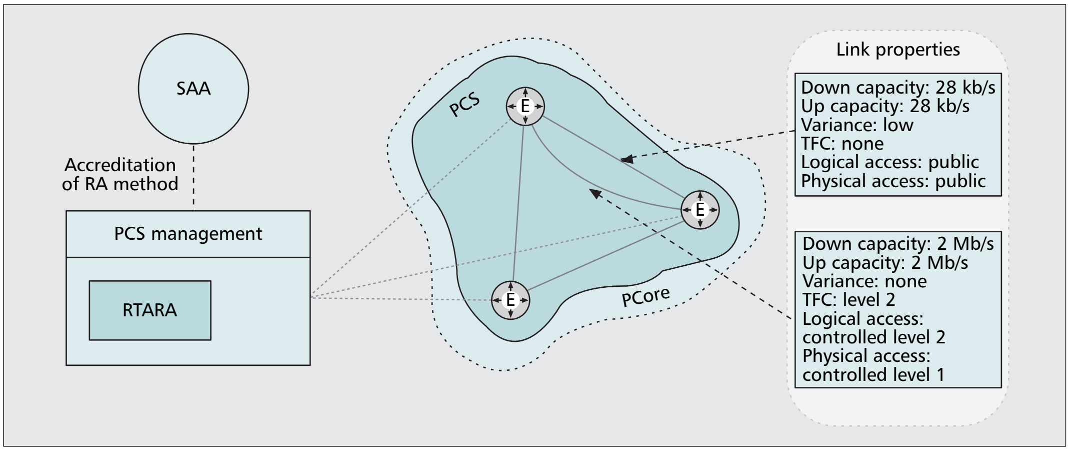


**Figure 3.** *Link properties are captured by the Es and reported to the management system where risk assessment is performed using a method approved by the SAAs involved.*

itation[4] of the PCS. The current process of accreditation is static and does not allow for quick adjustment. In order to overcome this, the SAAs should accredit risk assessment methods rather than a snapshot of a system at a given time. The continuous application of an accredited assessment method would be able to accredit (or reject accreditation of) the systems even in the presence of frequent changes. The role the SAA can play in PCN is illustrated in Fig. 3.

## Protected Core

In order to build a transport network from two or more PCSs such that it adheres to the principles of PCN, nations will have to work by a federation-of-systems approach. In the PCore that is thus established, a PCS should only be concerned with its direct neighbors. A cascaded management model [9] should be implemented to ensure delivery of services across multiple PCSs.

The services required at PCN-1 to ensure coherent service delivery across PCSs must be agreed on by the nations. In a federation of systems these services must implement a federated management and transport capability according to the parameters in a negotiated SLA.

### Federated Management

The interaction between PCSs over PCN-1 must include the setup and negotiation of SLAs as well as the exchange of management information that is useful to other segments such as information related to the risk level, security policies, and key management.

A determining factor in deciding which services will be offered to an interconnecting PCS is the risk level. Therefore, in the process of establishing an interconnection between PCSs, a measure of risk has to be mutually exchanged that reflects the current risk levels of these PCSs. The exchange does not require visibility of the neighboring PCS. Rather, it requires the SAAs of the nations involved to mutually recognize the risk assessment methodologies that are used. As the PCore changes, the risk assessment that is done per PCS might produce a different result. Based on this result, a PCS might want to renegotiate an SLA. In order to take full benefit of RTARA in a future PCN implementation, the current static process of SLA negotiation must be developed towards a more dynamic process.

The security policy enforced at PCS interconnection boundaries is dependent on the properties of the connecting PCS, and has to be negotiated on each interconnection. The policy must be adjusted if the SLA or risk levels change. The required interaction between security policy management, SLA management and the RTARA system is subject to further research.

A key aspect of federated management is the ability of the PCS management systems to exchange policy notifications in order to confine an attack to one PCS, or to render it futile at other access points to the PCore. This requires the development of a security policy language that can be interpreted by all PCS management systems involved.

In a PCore many kinds of encryption keys are involved, and although most of these keys relate to link protection and management internal to a PCS, federated key management is critical to allow authentication and interaction between PCSs, and it is a topic of further research.

### Transport Service

In providing transport service to CCs, a PCS might utilize other PCSs. Hence, the transport service must be able to handle different types of performance and security requirements. One such requirement is for CCs to have the ability to request a path through the PCore based on specific trust requirements, such as utilizing only PCSs under certain ownership.

### Dynamic Accreditation of a PCore

The PCore is a federation of systems, and there is no single authority that can accredit a PCore. Each nation performs dynamic accreditation of its own PCS, but the SAAs involved have to cooperate to collectively accredit the PCore, for example, by mutually recognizing the national risk assessment (RA) methods. This is illustrated in Fig. 4.

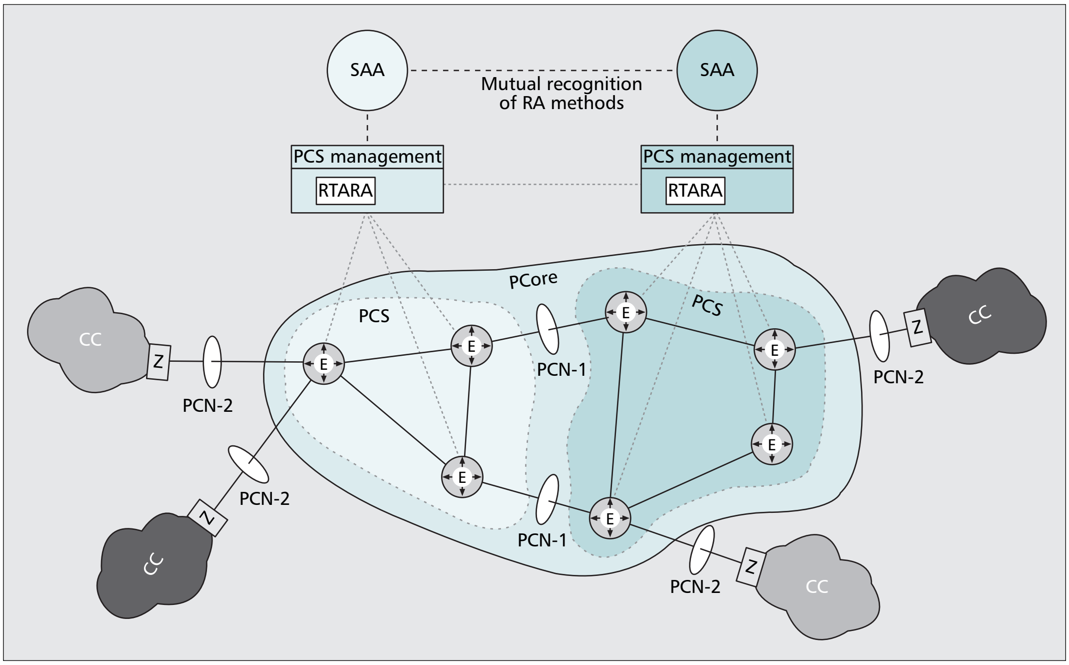
### Core Dynamics

The routing protocols in the PCore should support core dynamics (i.e., the addition or removal of PCSs, and their expansion or reduction). This

*The services that are required at PCN-1 to ensure coherent service delivery across PCSs must be agreed upon by the nations. In a federation of systems these services must implement a federated management and transport capability according to the parameters in a negotiated SLA.*

[4] *The security accreditation, or accreditation, of a network is a declaration by the SAA that the considered network operates in accordance with the envisaged security objectives, and that the induced residual security risk is known, accepted, and managed.*

In a PCore many kinds of encryption keys are involved and although most of these keys relate to link protection and management internal to a PCS, federated key management is critical to allow authentication and interaction between PCSs.



■ **Figure 4.** *The SAAs mutually recognize the RA methods so that dynamic accreditation of the PCore becomes possible.*

might be difficult with current technology where the principle is to route traffic at the lowest cost to the autonomous system, while in PCN the principle is to route based on optimal service delivery. External routing protocols that support more dynamic environments typically assume non-transport networks. However, the requirement for support of core dynamics exists at PCN-1; the CCs do not rely on fixed addresses, and address handling is fully controlled by the PCore. The topic of core dynamics in PCN is subject to further research.

## Definitions

The previous sections have emphasized the concept and benefits of PCN. For future reference, this section lists the definitions of the key terms in PCN:

- **A superior capability**: A robust capability that efficiently fulfils all the required needs.
- **The concept of protected core networking**: PCN is the concept of providing transport services in dynamic environments focusing particularly on achieving optimized availability. This is achieved by using multiple classes of network services for both performance and security, combined with superior knowledge, management and control, and protection of all network components.
- **Protected core segment**: A protected core segment (PCS) is a network built on the principles of PCN that is designed to work seamlessly with other PCSs in a federation of systems.
- **Protected core**: A PCore is a set of PCSs working together in a federation-of-systems approach to collectively achieve the characteristics of PCN.

The following interfaces, shown in Fig. 4, are defined by PCN:

- **PCN-1**: SIOP PCN-1 is the interface between PCSs in a PCore. PCN-1 is used to offer services and share all necessary management information between PCSs.
- **PCN-2**: SIOP PCN-2 is the interface between a PCS and a CC. PCN-2 is used to offer services to CCs and provide management information about these services.

## Required and Ongoing Work

The PCN concept is an architectural approach that fully supports an NEC environment. Approaches with similar components have been proposed or are being used to build current systems. The U.S. Global Information Grid (GIG) considers a black core approach [10], where all data is encrypted before entering the core, and the core can be shared between multiple classifications. However, unlike PCN, which separates information confidentiality from the protection of the core, the IP encryption in the black core approach is intended to do both. The loose coupling achieved with PCN-2 is therefore not achieved. Furthermore, the federated aspect is not a primary focus of the GIG black core, and it is not obvious that an equivalent of PCN-1 exists.

Another architectural approach is the NATO TACOMS approach [11], which focuses primarily on the federated interface between communications infrastructure (i.e., the equivalent of PCN-1). However, TACOMS does not clearly separate the transport of information from all information services, and the security requirements therefore become slightly different. TACOMS does not have a definition of PCN-2, and as such does not achieve support for seamless mobility.

PCN establishes a vision for future networking as well as postulates a number of concepts, services, and techniques that must be provided. Some of these concepts and techniques are well

| Established | | Cutting edge | | Novel | |
|---|---|---|---|---|---|
| **Concept** | **Techniques** | **Concept** | **Techniques** | **Concept** | **Techniques** |
| High availability<br>Multiple levels of precedence and preemption<br>Multiple traffic classes (converged network) | Enforcement techniques (e.g., authentication)<br>MPLS (supports, e.g., TFC as a service) | Availability in high-threat environments<br>Federated management<br>Integrated network and security management<br>Policy-based management<br>Seamless mobility<br>SLA negotiation | Dynamic group keying<br>(Supports seamless mobility)<br>IPsec discovery (Supports seamless mobility)<br>MLPP in packet networks<br>Policy-based routing (Supports e.g. TFC as a service) QoS | Capturing link security properties<br>Core dynamics<br>Core expansion<br>Dynamic accreditation<br>Federated military transport network<br>Loose coupling between CCs and PCore<br>Overlay of a protected layer<br>Real-time automated risk assessment<br>TFC as a service | Risk measure exchange (supports e.g., TFC as a service) |

**Table 1.** *Concepts and techniques of PCN grouped according to maturity (there is no link between terms in the same row).*

known and mature, others are being researched, and some are novel. Table 1 groups the concepts and techniques needed for PCN according to their maturity. Research and development should be focused on concepts and techniques in the novel category in order to properly support PCN.

## Conclusion

PCN is an approach to creating a transport network that is secure and flexible, properly supporting the requirements of an NEC environment. Such a transport network is necessary to enable proper information sharing and achieve the desired level of agility in operations. A number of concepts are utilized in PCN in order to achieve these effects.

A future implementation of the PCN concept can offer additional benefits to operational users and infrastructure operators, including a possible reduction in infrastructure, better utilization of current infrastructure, easier utilization of third-party communications, and automated risk assessment to aid in rapid accreditation of the system.

While some of the concepts and techniques necessary for PCN are available and well known, many are either immature or novel. Further work in these areas is necessary to reach a fully functioning PCN. This requires engagement of researchers in the field of network and communication systems.

## References

[1] D.S. Alberts and R.E. Hayes, “Planning: Complex Endeavors,” U.S. DoD Command and Control Research Program, 2007.

[2] D.S. Alberts and R.E. Hayes, “Power to the Edge,” U.S. DoD Command and Control Research Program, 2003.

[3] T. Szigeti and C. Hattingh, *End-to-End QoS Network Design: Quality of Service in LANs, WANs, and VPNs*, Cisco Press, 2004.

[4] K.I. Park, *QoS in Packet Networks*, Springer Science, 2005.

[5] R. Goode *et al.*, “Attaining Precedence-Based Communications in Secure IP Networks,” *Proc. MILCOM ’07*, 2007, p. 1.

[6] R. Yavatkar, D. Pendarakis and R. Guerin, “A Framework for Policy-Based Admission Control,” RFC 2753, Jan. 2000.

[7] G.M. Perez *et al.*, “Dynamic Policy-Based Network Management for a Secure Coalition Environment,” *IEEE Commun. Mag.*, vol. 44, pp. 58–64, Nov. 2006.

[8] D. Booth *et al.*, “Web Services Architecture,” W3C Working Group Note, Feb. 11, 2004; http://www.w3.org/TR/2004/NOTE-ws-arch-20040211

[9] D. McCarthy and P. Haraszti, “Specification of Inter-Domain Quality of Service Management Interfaces,” Euro. Inst. Research and Strategic Studies in Telecommun. tech. spec., Heidelberg, Germany, EDIN 0109-1008, May 2001.

[10] J. Tarr and T. DeSimone, “Defining the GIG Core,” *Proc. MILCOM ’07*, pp. 1–6, 2007.

[11] B. Hughes and T. Sharpe, “NATO TACOMS,” *Proc. MILCOM ’07*, 2006, pp. 1–7.

## Biographies

GEIR HALLINGSTAD (geir.hallingstad@nc3a.nato.int) received his B.Sc. and M.Sc. in computer engineering from Iowa State University in 1996 and 1997, respectively. He has over 10 years of experience working with information security in military systems and is currently working as a principal scientist at the NATO C3 Agency. His primary focus is networked systems that provide both secure and flexible communications in support of an NEC operational environment.

SANDER OUDKERK (sander.oudkerk@nc3a.nato.int) is a senior scientist in information assurance at the NATO C3 Agency in the Netherlands. He has over eight years of experience in commercial, government, and military information security. His research interests include network security, cross-domain sharing solutions, and security services in federated networks. He received an M.Sc. degree in mathematics from the University of Utrecht, the Netherlands, in 2000, and is a member of the IEEE Computer Society.