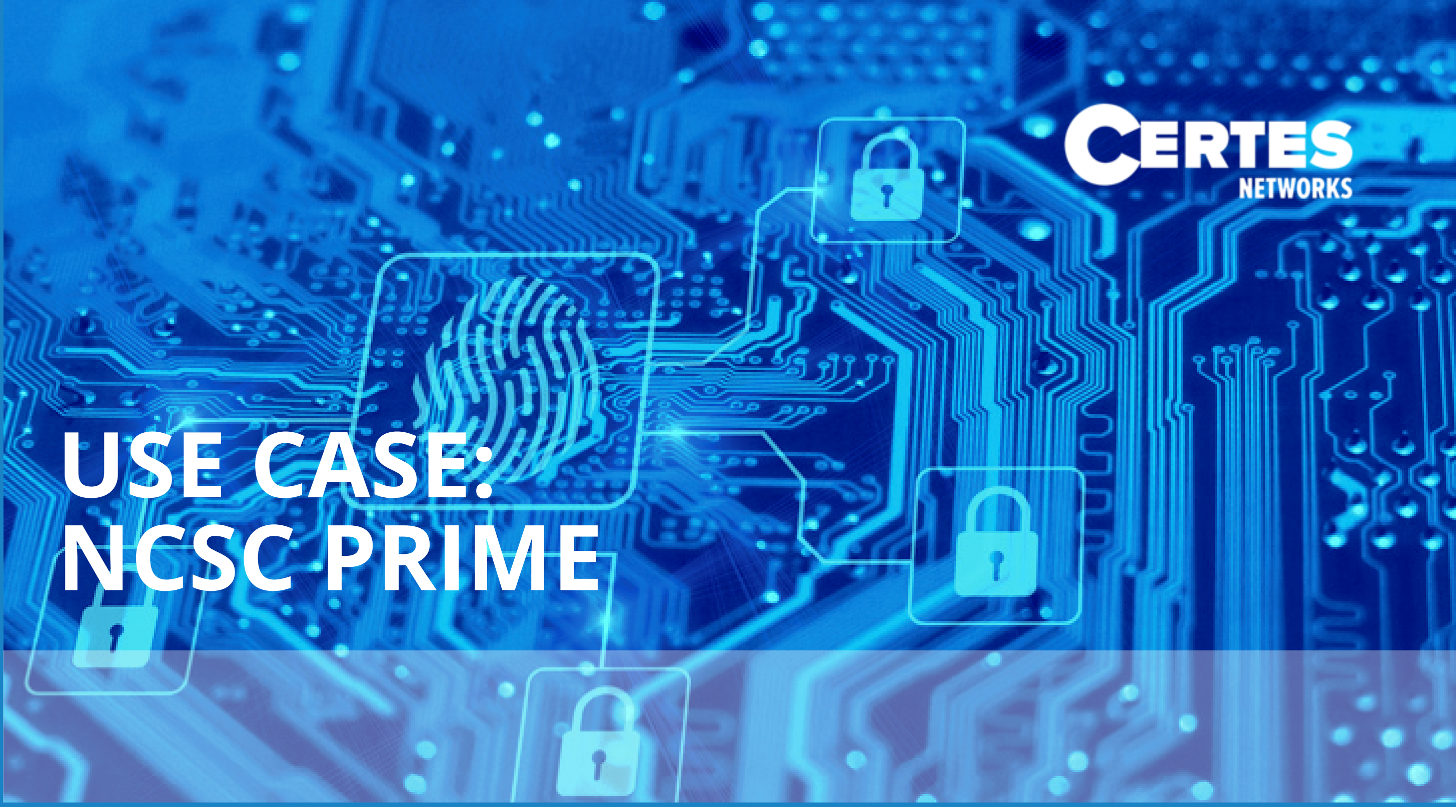

USE CASE: NCSC PRIME

SITUATION ANALYSIS

The National Cyber Security Centre (NCSC) has provided guidance designed to help UK users to deploy or buy network encryption, using IPsec. The recommended IPsec cipher suite profile outlined in this Use Case is for protecting information – this is also known as PRIME.

This guidance is not just for Public Sector, it's for all UK businesses and closely correlates to GDPR obligations. However, Public Sector has little choice but to follow recommended NCSC guidelines. It provides minimum recommendations for the selection and configuration of relevant equipment. It also describes how a network encryption service needs to operate to provide an understood level of security.

The NCSC standards were designed for the protection of information flows within a single organisation, or within a group of organisations, across bearer networks such as the Internet, a commercial WAN circuit, or the Public Services Network (PSN) for public sector organisations.

The guidance as published is based on the network vendor being CAS(T) certified (CESG (Communications Electronics Security Group) Assured Services (Telecommunications)), which involves an independent assessment focused on the key security areas of service availability, insider attack, unauthorised access to the network and physical attack.

CHALLENGES

1 PUBLIC SECTOR ADHERENCE TO CAS(T)

Many Public Sector organisations are no longer mandating CAS(T) based services and therefore the risk appetite is expected to be lowered, mainly to support the emergence of internet and SD-WAN suppliers network solutions. This is key as the Foundation standards for IPsec, also referenced below, will expire sooner than 2023 and users are being encouraged to move quickly off legacy platforms.

2 IMPACT TO CLOUD SERVICE PROVIDERS AND BEARER NETWORKS

This guidance, such as the protection of information flows on dedicated links between organisations, also applies to cloud service providers, or in the inter-data-centre connections in such providers' networks. The underlying bearer network is assumed not to provide any security or resilience. This means that any bearer network (such as the Internet, Wi-Fi 4/5G, or a commercial MPLS network) can be used. The choice of bearer network(s) will have an impact on the availability that an encrypted service can provide.

3 WHEN IT COMES TO PARTNER COLLABORATION

NCSC explicitly states in its guidance that establishing trustworthy encrypted network links is not just about technology. It is also important that the management of these network links is carried out by appropriate individuals, performing their assigned management activities in a competent and trusted fashion, and from a management system that protects the overall integrity of the system.

Thus, for encryption solution providers, like Certes Networks and others, who we partner with and the partner's service credentials impacts how the end user may use our technology.

SOLUTION REQUIREMENTS

IPsec helps protect the confidentiality and integrity of information as it travels across less-trusted networks. Network-based encryption is implemented using the IPsec protocol to establish Virtual Private Networks (VPNs). This can be performed by a software client running on an End User Device (EUD), by a dedicated hardware appliance (a VPN gateway), or as additional functionality in other networking infrastructure equipment (such as a router).

IPsec VPNs may be dedicated to a single purpose (such as two gateways which connect data centers together.) Alternatively, a single gateway may be used by multiple clients as required (for example, for remote working connections).

Basic NCSC PRIME Principles

Devices which implement cryptographic protection of information using IPsec should:

- Be managed by a competent authority in a manner that does not undermine the protection they provide, from a suitable management platform
- Be configured to provide effective cryptographic protection
- Use certificates as a means of identifying and trusting other devices, using a suitable PKI
- Be independently assured to Foundation Grade, and operated in accordance with published Security Procedures
- Be initially deployed in a manner that ensures their future trustworthiness
- Be disposed of securely

Keep the network design simple

Keeping the network design simple is one of the most effective ways to ensure the network provides the expected security and performance. With this in mind:

- Avoid the need for too much security functionality in any single product or network feature, as a failure in one will likely compromise all.
- VPN gateways should ideally have three interfaces; a LAN-side interface which has plain-text traffic on it, a WAN-side interface with IPsec-encrypted data, and a management interface (which may be local, or WAN-connected with suitable encryption).
- End User Devices should have a single WAN interface.
- Some network designs may use multiple LAN or WAN interfaces, as well as traffic routing rules at layers 2 - 4 which cause data either to be passed in-clear or to be encrypted (based on traffic characteristics such as destination IP address / port / VLAN ID etc). However, adding additional complexity to the network design increases the risk that traffic will be mis-routed, or that devices will become misconfigured, allowing an attacker access to them (and the data they protect). If such routing represents a security barrier in the network design, then the devices performing this function should have had it included in their evaluation.

Recommended cryptographic profiles

As a default policy, VPN gateways and clients should be configured to offer and accept only Foundation and PRIME profiles and should not allow negotiation of alternative cipher suites unless explicitly permitted by an administrator.

- For public sector organisations, use of the previous 'PSN Interim' profile remains acceptable until 31st December 2018 for the purposes of maintaining existing services, and enabling the transition to the above profiles.
- NCSC recommended that all IPsec VPNs migrate to use of the PRIME or Foundation cryptographic profile by 1st January 2018.
- The Foundation Profile is expected to provide suitable protection for OFFICIAL information until at least 31st December 2023. This date will be reviewed on an annual basis, with a yearly extension on continued acceptability as appropriate. Use of Untrusted Bearers that are not CAS(T) based means that Foundation cannot be used
- Depending on equipment and infrastructure support, deployment of either the Foundation or PRIME profile is acceptable.

The recommended algorithms and key sizes for root and sub-CAs used to issue certificates for end entity devices are:

Profile	Details
Foundation	2048-bit RSA and SHA-256
PRIME	ECDSA-256 and SHA-256

PRIME profile for IPsec

The recommended IPsec cipher suite profile for protecting information is called PRIME. A non-authoritative summary is provided in the table below:

IKEv2	Selection
Encryption	AES-128 in GCM-128 (and optionally CBC)
Pseudo-random function	HMAC-SHA256
Diffie-Hellman Group	256bit random ECP (RFC5903) Group 19
Authentication	ECDSA-256 with SHA256 on P-256 curve

ESP	Selection
Encryption	AES-128 in GCM-128

Authoritative reference: CESG Technical Specifications No. 403 - PRIME Framework - Suite B.128 Module. Issue 1.2.2 November 2012

Foundation profile for IPsec (Note Legacy)

This profile consists of an RFC-compliant implementation of IPsec with IKEv1 (RFC2408 and RFC2409 apply), without custom extensions, using Extended Sequence Numbers (RFC4304), Encapsulating Security Payload (ESP - RFC4303), and the algorithms given in the tables below:

IKEv1	Selection
Encryption	AES with 128-bit keys in CBC mode (RFC3602)
Pseudo-Random Function	HMAC-SHA-256 (RFC4868)
Diffie-Hellman Group	Group 14 (2048-bit MODP Group) (RFC3526)
Authentication	X.509 certificates with RSA signatures (2048 bits) and SHA-256 (RFC4945 and RFC4055)

ESP	Selection
Encryption	AES with 128-bit keys in CBC mode (RFC3602)
Integrity	SHA-256 (RFC4868)

IKE phase 1 MUST use Main mode. SA lifetimes must be 86400 seconds (1 day) for Phase 1 and 28800 seconds (8 hours) for Phase 2.

Certain network functionality may require deviation from this profile. It is acceptable to replace any element of the Foundation profile with the corresponding element from the PRIME profile (for example, using IKEv2 instead of IKEv1). Until the transition date below, if interoperability is required, the Foundation profile should be used.

Certificates

For most IPsec-based networks, VPN gateways and clients will need to use certificates based on a central trust infrastructure to successfully identify themselves to other VPN devices. NCSC has guidance on the use and management of certificates.

NCSC does not recommend using Pre-Shared Keys (PSKs), Group Domain of Interpretation (GDOI), and other approaches for establishing shared keys across multiple devices. However, NCSC recognises that Pre-Shared Keys are widely used in site-to-site VPNs. In this case we recommend that keys are generated in a cryptographically secure manner to ensure that they have a high level of entropy to help mitigate brute force attacks.

THE SOLUTION

CERTES NETWORKS TECHNOLOGY IS PRIME COMPLIANT

Certes Networks WAN encryption management solution is PRIME compliant. Certes encryption hardware and software technology can seamlessly integrate with SD-WAN without disrupting or impacting the current network infrastructure. And, our technology is not only compliant with PRIME but more advanced than the mandatory requirements themselves.

The Certes Network Layer 4 solution is the ideal solution for those public agencies and Federal governments who want to move from Legacy MPLS to an SDN or SD-WAN architecture. And with NCSC starting to treat all networks as untrusted networks (especially those agencies using internet), PRIME is becoming the gold standard for which NCSC will measure regulatory compliance.

CERTES NETWORKS

Contact Certes Networks

300 Corporate Center Drive, Suite 140
Pittsburgh, PA 15108

Tel: 1(888)833-1142
Fax: 1(412)262-2574

info@certesnetworks.com
sales@certesnetorks.com

We offer an encryption solution that is simple, scalable and uncomplicated.