Annex 5. Blueprint Architecture

This annex aims at setting a blueprint architecture for this initiative. It should not be meant as mandatory top-down implementation guide, but as an effort to harmonise jargon, functionalities and approaches.

For the purpose of this proposal, it is considered that many SOCs and cybersecurity networks or teams are already in place in the MSs, and that each MS organises its own network of SOCs as it wishes. Therefore, for the purpose of this document each MS is a black box. In the end, it is only expected that each MS should designate a single point of contact that would interact with the rest of the network: the MS's national SOC.

This annex is organised as follows. Section 2 details the building blocks composing a national SOC. Section 3 presents the general overview of the EU network of SOCs. Finally, Section 4 details the functionalities of the network.

1. Building blocks of a national SOC

A national SOC can be defined as a centralised security organisation that assists companies and organisations of a MS in identifying, managing, and remediating distributed security attacks.

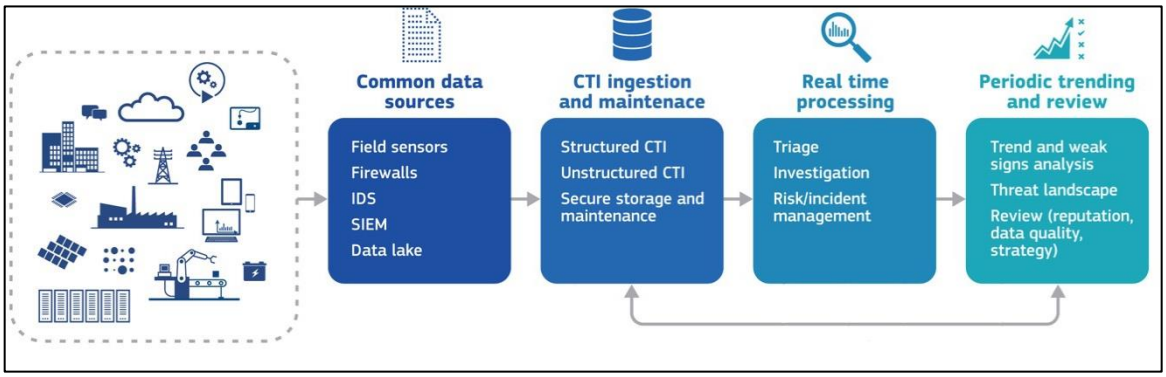

Figure 1. Building blocks of a national SOC.

From a functional point of view (Figure 1), it is generally composed of four building blocks:

- common data sources (public or private sector, such as national CSIRTs, vendor products, self-made internal IT systems or companies, social media and (dark) web, sectorial CERTs or Information Sharing and Analysis Centres (ISACs).
- CTI ingestion and maintenance: to remodel unstructured collected data into structured ones and help the SOC to assimilate the collected data correctly and to build a clean data set of CTI.
- real time processing (to detect anomalies, correlate events etc.)
- periodic trending and review (to assess the quality of the data collected, identify high-level trends or global threats).

These elements do not need to be all present in a national SOC at the moment of the launch of this initiative, however, they can be understood as the functionalities which every SOC should tend to have in the long run.

2. General overview of possible cross-border architectures

As highlighted in the previous section, every MS is free to organise its internal network of SOCs as it wishes: the architecture of the national networks of SOCs is a black box from the point of view of the EU network of SOCs. Each

MS participating to this EU network should designate a **national SOC** that will act as a proxy between its own national network and the rest of the EU network, and in case, also as coordinator which will partake in a joint procurement foreseen by this initiative.

The participating MSs can be grouped by **consortium** that may, for instance, cover specific geographical areas of the EU, and provide CTI to relevant entities in their area of operation. Each consortium must develop a **cross-border SOC platform** to allow the national SOCs of its participating MSs to communicate together and disseminate their collected information via sharing and reporting CTI or cybersecurity incidents.

The various consortia are then interconnected together via a dedicated cross-border **gateway** in order to share their aggregated CTI or cybersecurity incidents. They would form the EU network of SOCs.

This section presents the two architectural layers of the network:

- The *lower layer*, at the level of the consortia (how the MSs of the consortium are organised among themselves),
- The *upper layer*, at the level of the EU network of SOCs (how the interoperability and sharing is guaranteed among the various consortia participating to the network).

2.1. Topological structure of the lower layer

The topological structure of a consortium interconnecting different MSs (each MS having its own national SOC) can be essentially of three types, namely centralised, decentralised or fully distributed. Figure 2 depicts these three topologies.

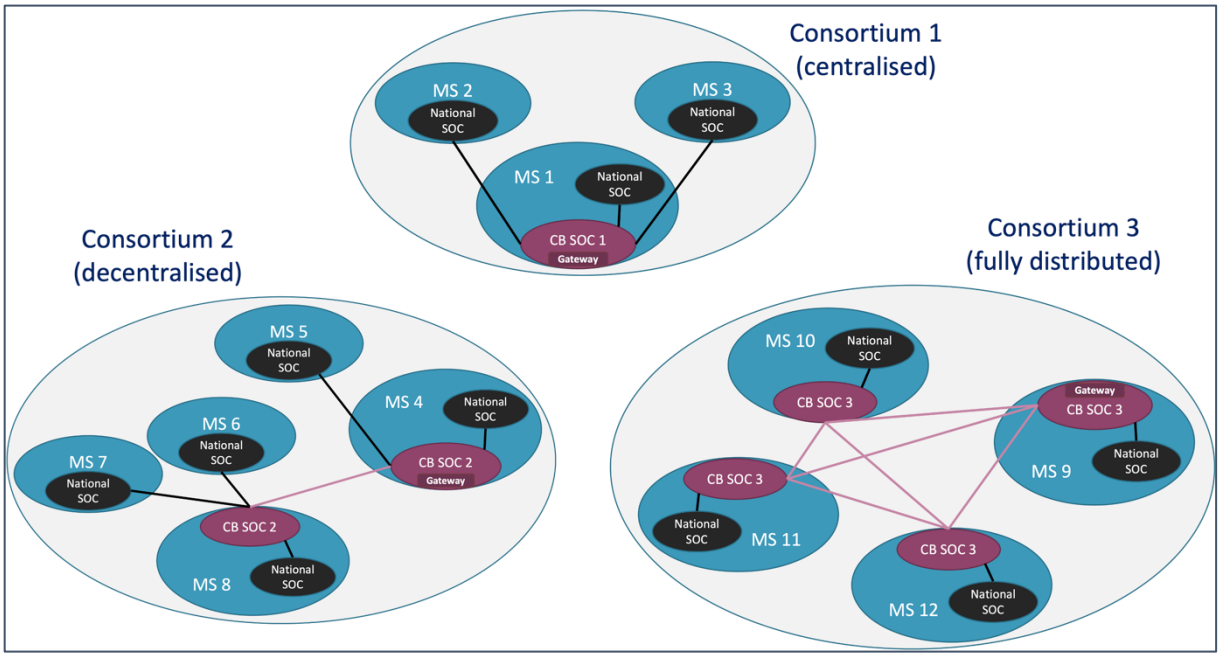

Figure 2. Different topologies of architecture for consortia.

In a **centralised** architecture, data and operations are at a central location. A designated MS hosts the entire cross-border SOC platform and gateway to collected and share the CTI of the consortium with the rest of the network.

In a **decentralised** architecture, few core or "central" nodes (geographically distributed) share information directly among themselves and they are surrounded by their local satellite nodes.

Finally, in a **fully distributed** architecture, a consortium is similar to a full peer-to-peer network where each MS hosts a part of the cross-border SOC platform in order to communicates with all the others. As for the other topologies, one designated MS also hosts the gateway to collected and share the CTI of the consortium with the rest of the network.

The long-term goal of this initiative is to ensure that information flows not only among entities of the same consortia, but also across different consortia.

2.2. Topological structure of the upper layer

The topological structure of the proposed EU network of SOCs interconnecting different cross-border SOC gateways (each consortium having one gateway) can be essentially of two types: centralised or fully distributed. Figure 3 depicts these two topologies.

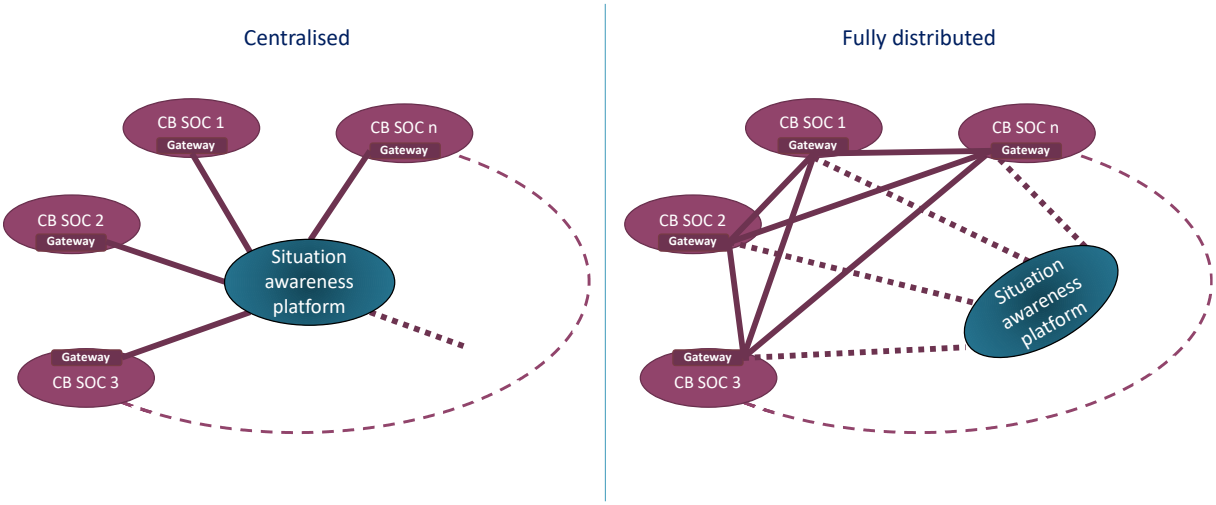

Figure 3. High level view of the different topologies of architecture the EU network of SOCs.

3. Functionalities of the network

The proposed EU network of SOCs must put in place a certain number of mandatory functionalities in order to provide the best results possible in terms of cybersecurity. This section details these mandatory functionalities: sharing, aggregation, correlation, reporting, dashboard crowding, and security.

Figure 4 provides a complete overview of the network with the centralised topology[1]. It further highlights the location of the functionalities within the network (i.e., which component must implement which functionality). Note that the “security" functionality must be implemented everywhere in the network, and therefore it is not depicted in the figure.

[1] The figure of the network with the fully decentralised topology is the same figure without the situation awareness platform.

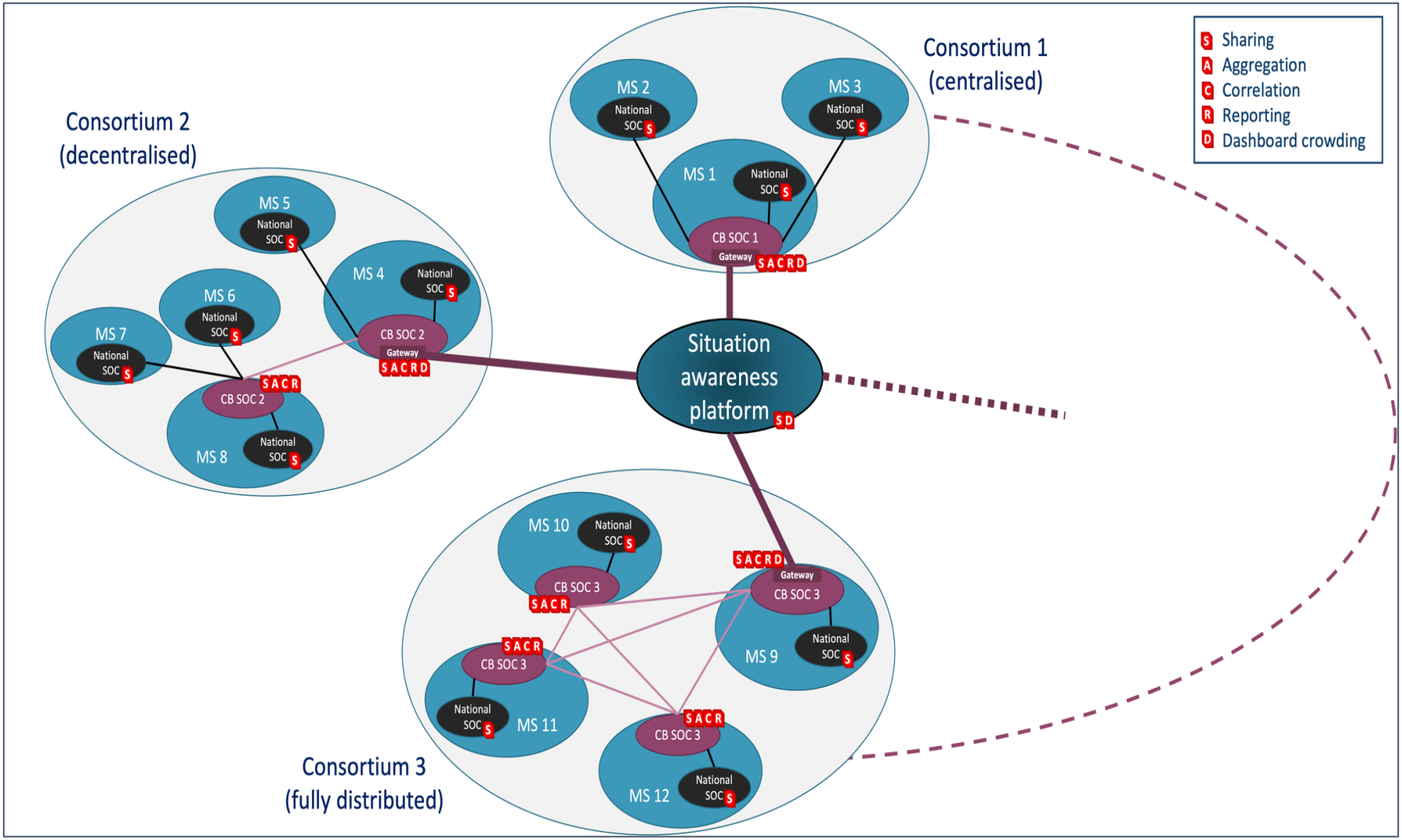
Consortium 1
(centralised)
Consortium 2
(decentralised)
Consortium 3
(fully distributed)
S Sharing
A Aggregation
C Correlation
R Reporting
D Dashboard crowding
MS 1
MS 2
MS 3
MS 4
MS 5
MS 6
MS 7
MS 8
MS 9
MS 10
MS 11
MS 12
National SOC
CB SOC 1
CB SOC 2
CB SOC 3
Gateway
S A C R D
S A C R
Situation awareness platform
S D

Figure 4. Full overview of the proposed EU network of SOCs with the mandatory functionalities.

4. Security

As the network will share potentially sensitive information, security of the data at rest and in transit is paramount.

In all the various network architectures described previously, it is necessary to define common security requirements. The different national SOCs need to exchange data with each other, meaning that they should be able to put in place bidirectional communication. With a centralised topology, there would be a main central cross-border SOC platform collecting information, but this information could be redistributed to regular nodes which should therefore be able to both send and receive data in a secure manner. This is even clearer in case of decentralised or fully distributed topology. SOCs need to act both as client and server for information exchange. Figure 5 gives an overview of the high-level fully distributed architecture interconnecting three SOCs of three different MSs.

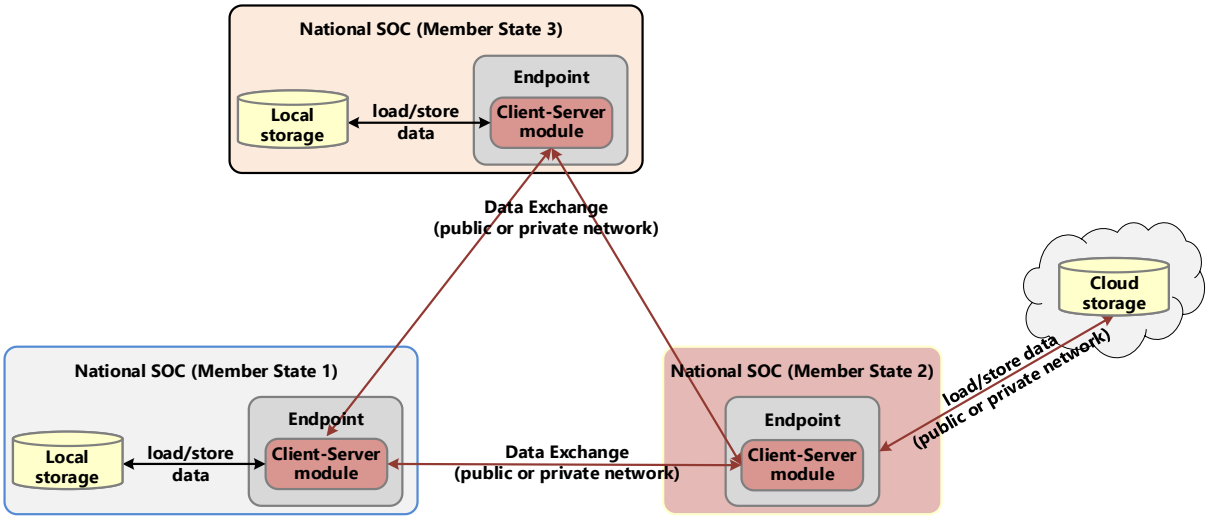

Figure 5. High level architecture for SOCs interconnection

4.1. Security of networks and communications

Exchange of data between two endpoints of two different national SOCs needs to be secured. The communication can take place over unsecure channels (e.g., the Internet), so it is fundamental to apply security measures at different layers of the Open Systems Interconnection (OSI) model[2]. An alternative to public networks could be the use of the current version of the Trans European Services for Telematics between Administrations (TESTA-ng), which already interconnects some public administrations and offers security features.

Protection of communications should rely at least on Transport Layer Security (TLS) protocol and on asymmetric cryptography. With asymmetric encryption, each endpoint would be responsible for the security of its private key, which should be stored in a tamper-proof device such as a Hardware Security Module (HSM) or a smart card.

The measure above however does not guarantee confidentiality of network interactions, i.e., information that could be revealed at the network layer of the OSI model for example by the IP packet headers (e.g., type of transport protocol, addresses). A solution for this could be the realization of a site-to-site Virtual Private Network (VPN) between the different network gateways in the national nodes, for example leveraging on the Internet Protocol Security (IPSec) suite of protocols to implement network tunnelling.

A supplementary measure could be the choice of implementing application layer encryption, thus providing end-to-end security at the highest point of the network stack, i.e., at user level.

[2] Standard ISO/IEC 7498.

4.2. Security of data-at-rest

Data should not be kept in plain in the data storages. Data storages should be encrypted with the state-of-the-art algorithms, and encryption keys protected and managed using tamper-proof devices. The encryption could be implemented by the application sharing data with the others, left to specific features of the database software, or realised through disk encryption functionalities. In all the cases above, it must be highlighted that storage encryption can introduce performance reduction and additional management overhead, for example when nodes reboot. Therefore, due care is necessary when selecting the solution according to the specific scenario and context.

4.3. Credentials management

Previous sections mention the use of digital certificates and of public and private keys in the context of asymmetric cryptography. Creation, distribution, and management of these electronic credentials need to be assigned to a Public Key Infrastructure (PKI), and therefore to a Certificate Authority (CA) issuing the digital certificates. The strengths and reliability of the PKI is of utmost importance, with possibility to rely on public or private PKIs

A crucial step in the issuance is the identification of the entities that have access to the system and secure delivery of credentials to them. As already said, each entity should generate its own key pair and a request to sign its certificates. The pair should be generated directly on a smartcard or HSM so that the private key never leaves the tamper-proof device. The public key extracted to generate the certificate that would be signed using the CA's root private key. The latter is a crucial aspect whose protection again should be entrusted to an HSM device. It is important that deliveries of certificates to a user are done with no intermediaries, and that the support (typically the smartcard) is protected by an authentication factor (e.g., a PIN) which is delivered through another channel and always kept separately from the support itself. Secure architecture

The introduction of the security measures described in the previous sections, brings to a refinement and enrichment of the high-level architecture depicted in Figure 5. Those changes reflect the presence of the different security components, such as digital certificates, key pairs, and gateways for network traffic encryption. This brings to a secure architecture shown in, that indeed puts in place both TLS and VPN encryption for two layers of protection in the exchange of data.

Figure 6 provides an example of the integration of all the elements described in this section.

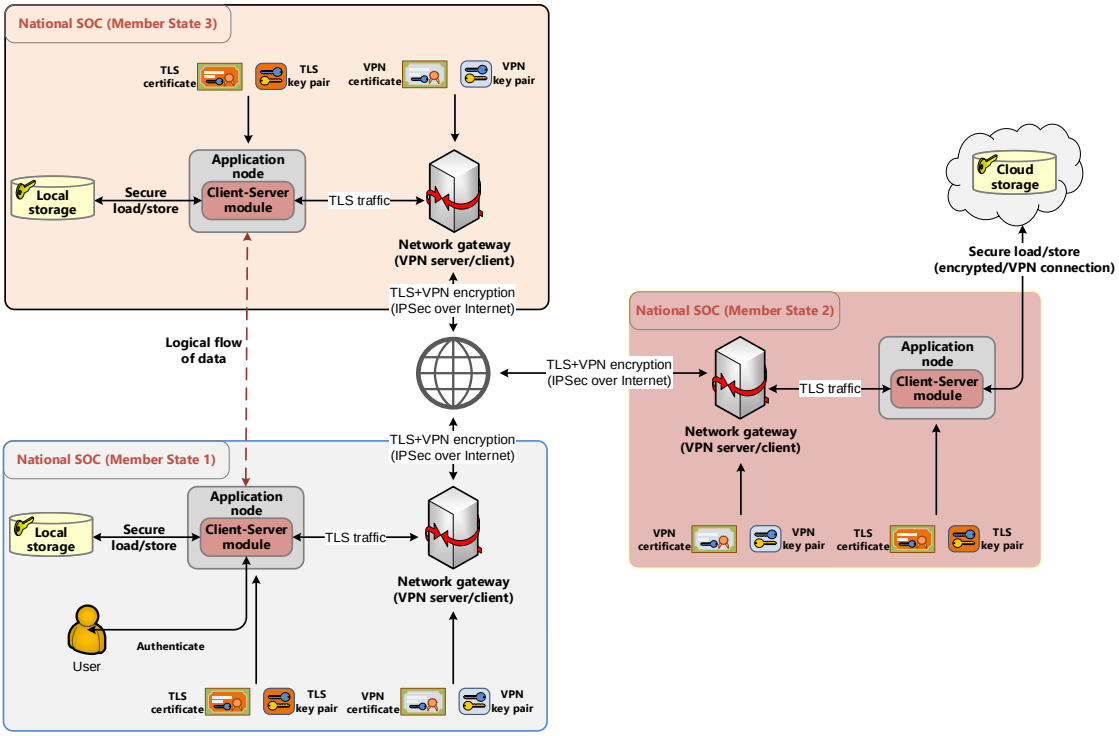

Figure 6. Secure architecture for SOCs interconnection.