An Interoperable Zero Trust Federated Architecture for Tactical Systems

Alexandre Poirrier, Laurent Cailleux, Thomas Heide Clausen

▶ **To cite this version:**

Alexandre Poirrier, Laurent Cailleux, Thomas Heide Clausen. An Interoperable Zero Trust Federated Architecture for Tactical Systems. MILCOM 2023 - 2023 IEEE Military Communications Conference (MILCOM), 2023, pp.405-410. ⟨10.1109/MILCOM58377.2023.10356247⟩. ⟨hal-04364111⟩

HAL Id: hal-04364111

https://hal.science/hal-04364111v1

Submitted on 26 Dec 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Distributed under a Creative Commons CC BY-SA 4.0 - Attribution - ShareAlike - International License

An Interoperable Zero Trust Federated Architecture for Tactical Systems

Alexandre Poirrier
École polytechnique &
Direction Générale de l'Armement
Palaiseau, France

Laurent Cailleux
Direction Générale de l'Armement
Rennes, France

Thomas Heide Clausen
École polytechnique
Palaiseau, France

***Abstract*—In military and tactical missions, operational needs can require different domains and nations in a coalition to federate, to facilitate sharing of resource between domains. On the other hand, data and services need to be protected against unauthorized access. The zero trust paradigm provides principles for securing data and services, based on fine-grain compartmentalization of resources and least-privileged access policies. In zero trust architectures, every access to a resource is verified, without relying on implicit trust between the requester and the resource. However, state-of-the-art federation procedures weaken the zero trust security guarantees, as information on requesters, belonging to one domain, cannot be verified by another domain offering a resource. Therefore, access inherently relies on trust between domains, which contradicts zero trust principles.**

This paper presents a novel technique to create a zero trust federation, in which every access to a resource is explicitly verified, without trusting federation partners. In particular, due to the power constraints on devices composing tactical architectures, the presented solution does not require invasive software to be installed in requester devices.

***Index Terms*—Federation, Internet of Military Things, Software-Defined Perimeters, Zero Trust**

I. Introduction

Tactical networks for military operations are heterogenous: They have different objectives, *e.g.*, surveillance, reconnaissance, or tactical mission execution, and are composed of different devices, such as satellites, sensors, Unmanned Aerial Vehicles (UAV), or battleships. They also carry heterogenous communication, such as voice, video, or text [1]. They combine different technologies, such as combat-net radio (CNR), mobile networks (LTE), or satellite networks reaching Low Earth Orbit (LEO) satellites.

Devices in military architectures can be classified into different categories [2]. Resource-constrained devices have low computing power and battery, and can be deployed directly on the battlefield. Other components, such as computers in a command center or in battleships, dispose of an intermediate computing power, but also have an intermediate latency for processing information from the battlefield. Finally, military cloud services can be deployed to benefit from higher computing power, at the expense of higher latency. This is illustrated in figure 1.

A need for interoperability: During the Afghanistan intervention, the necessity for a coalition mission network to share information between allied nations arose. A first level of interoperability was reached with the Afghanistan Mission Network (AMN), facilitating decision making by enabling access to more complete information [3]. In 2012, the NATO Military Committee proposed an approach to improve the level of interoperability provided by the AMN, called Federated Mission Network (FMN) [4]. Widely accepted by NATO nations, the NATO FMN Implementation Plan (NFIP) was designed, and the fourth version endorsed in 2015 [5]. The need for interoperability has been confirmed to be fundamental for armed forces by NATO leaders in 2016 [6].

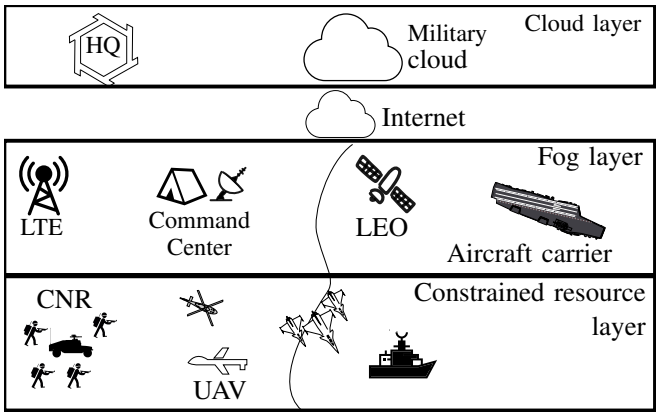


Figure 1: Base tactical architecture of a federation participant.

FMN aims at creating policies, procedures, and components for sharing data and applications, between Alliance nations and partners, and amongst communities of interest. The FMN consists of three parts: a framework, serving as a template for mission networks, a number of mission network instances, and a governance overseeing the framework and the specific mission network instances. The NFIP describes how to have interoperability in military networks, by proposing a service-oriented architecture. Development is staggered into several 'spirals', which add more capabilities providing interoperability between nations at operative and tactical levels [5].

Moreover, a need for Multi-Domain Operations (MDO) has been identified by NATO, which expands the requirements for interoperability across the five operational domains and between nations [7].

A need for security: Perimetric security is vulnerable to insider threats, and to lateral movements. These considerations, and the plethora of breaches from the 2010s, gave rise to the concept of 'deperimeterization', from the Jericho Forum in 2004 [8], and then the zero trust architecture, introduced by Forrester in 2010 [9]. This paradigm change has been adopted by the U.S. Department of Defense (DoD) with the 'Black Core' architecture [10] in 2007.

Following the Solarwinds attacks in 2020 [11], the U.S. government has made the transition to zero trust compulsory [12] [13], requiring federal agencies to meet zero trust standards by the end of the year 2024.

The goals of zero trust architectures are to secure and protect information, systems, and infrastructures against malicious activities, including organization information on non-owned networks [14]. This implies that several principles are to be followed by zero trust architectures [15], [16]:

1) **Authentication**: every entity (user, device, application, etc.) accessing resources needs to be authenticated;
2) **Least-privilege, per-session, and dynamic authorization**: access to resources is granted following a least privilege policy, for a limited time, with authorization taking into account contextual and environmental information;
3) **Segmentation of access and encryption**: access to resources is evaluated for smallest possible pieces, and communication to resources is always secured.
4) **Monitoring**: the infrastructure, entities, and resources are constantly monitored for improving security.

According to the [15], every resource is to be protected by a Policy Enforcement Point (PEP). As depicted in figure 2, every connection request is evaluated by a Policy Decision Point (PDP), which grants or denies access to the resource, by considering information on the requester, the environment, and threats. The decision of the PDP is enforced by the PEP.

Additional information considered by the PDP is provided by supporting components. Authentication is performed with an ID management (IdM) system, responsible for the identity of every entity and device in the organization. Identity refers to the set of attributes that describe entities and devices within a given context [17]. IdM systems can rely on other systems, such as a Public Key Infrastructure (PKI), to associate artifacts, such as certificates, with entity identities.

Moreover, every asset and device of the architecture is continuously monitored. This can be performed using a continuous diagnostics and mitigation (CDM) system [18], which collects security information on devices in the infrastructure, and a security information and event management (SIEM) system [19], which analyses security events collected by the CDM [15].

In tactical architectures, devices with low computing power may not be able to evaluate connection requests. In that case, the PDP can be an external process running in the fog layer.

Problem statement: Zero trust implies that every access to a resource needs to be verified, and that access must not be granted based on implicit trust.

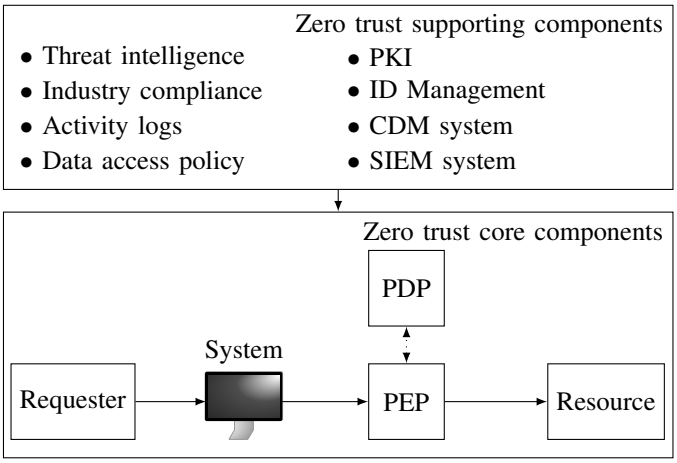


Figure 2: Zero trust architecture [15].

However, in a federation, every domain is responsible for authenticating and monitoring its own entities and devices. Therefore, if an entity requests access to a federated resource, information describing this entity, its devices, and its context, is provided by the requester domain, and the resource domain needs to trust that information. This weakens zero trust security guarantees, as granting access requires implicit trust between federation members [20].

Thus, this paper explores how it is possible to create a zero trust federation, in which every access to a resource is explicitly verified, without implicitly trusting federation partners.

A. Related Work

Interoperability of tactical systems: The FMN ensures interoperability between domains by enforcing standards, common to every architecture in the federation. This is the goal of the NATO Interoperability Standards and Profiles (NISP) [21].

Similarly, international standards are designed by the Multilateral Interoperability Program (MIP), a military standardization body composed of nations, of the European Defense Agency, and of NATO [22].

For enabling legacy systems to meet federation standards, legacy traffic can be encapsulated or converted by middle components. This allows minimal changes from original architectures, at the expense of higher operational latencies [23].

Another strategy for interoperability in tactical networks is Software-Defined Networking (SDN), which offers advanced management features [24]. This strategy is still a work in progress, with multiple research initiatives for overcoming challenges regarding heterogenous, multi-bearer networks with unpredictable service demand [2].

Zero trust federations: The possibility to create a zero trust architecture that can be federated with other architectures, zero trust or not, is evaluated in [25] for the U.S. Air Force. Six solutions are proposed. In the first four, called ZTE Federation, ZTE-like Federation, Identity Credential Federation, and Weak Identity solutions, the information describing the requester and

its device are provided by the requester domain, and trusted by the resource domain. The difference between those four architectures is the zero trust maturity of the federated architecture: a more advanced maturity provides higher security guarantees. The Ad Hoc Federation involves a central source, which determines which resource can be shared with which entity. Similarly, the Person-to-Person sharing enables users to share data with other users following a chain of command.

There are three solutions for providing zero trust in a federation, without trusting federated members [26]:

1) Installation of a trusted component in every device accessing resources, including devices from partners, to evaluate the security posture of devices.
2) Standardized hierarchical trust architecture: trust in other domains comes from trust in a supervising organization.
3) Third-party negotiation: a trusted third-party collects and shares information on every architecture.

A federated zero trust architecture is proposed by [27] following the third of the solutions. In this architecture, a third party, called the Context Attribute Provider (CAP), installs an agent on every device of federated architectures, and monitors those devices. The CAP can then be used by PDP to provide contextual information in access requests. The CAP can be split into two components, one component responsible for contextual information collection, and another component for contextual information exploitation [28].

B. Statement of Purpose

Existing solutions for federating zero trust architectures either require trust in a third party or in partners, or employ invasive techniques such as the installation of monitoring software on every device.

The former solutions imply an inherent trust, which is never challenged during the execution of the mission. This is in opposition with the zero trust principles, stating that access requests need to be verified. Moreover, in the military context of the FMN, the need for sovereignty and control of equipment prevents the use of intrusive techniques and the establishment of trust between nations, or in a third party.

This paper presents a non-intrusive federation of architectures, which ensures interoperability between federated domains while following zero trust principles.

C. Paper Outline

The remainder of this paper is organized as follows. Section II presents an abstract solution to federate zero trust architectures, which uses a component called remote attestation. Section III illustrates the federation of architectures with a Software-Defined Perimeters (SDP) based example architecture. Section IV concludes this paper.

II. A Proposed Federated Zero Trust Architecture

This section proposes a framework for how several architectures, following zero trust principles, as presented in figure 2, can federate. The basic idea is as follows: Each domain in the federation operates independently, and manages the identity, authentication, and monitoring of their infrastructure, devices, and entities, and control access to their resources.

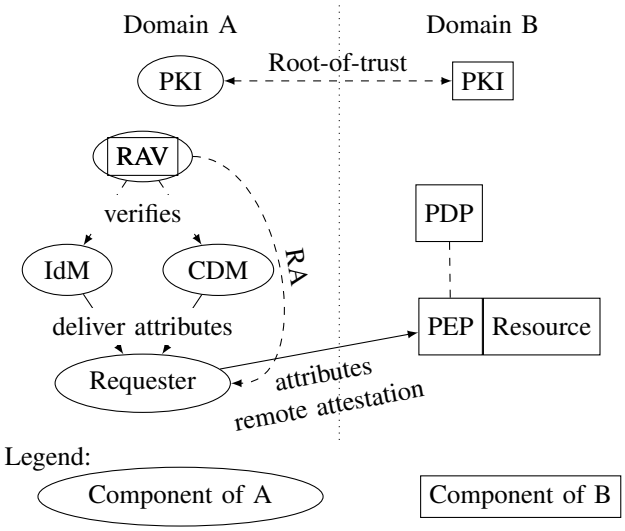


Figure 3: Proposed zero trust federated architecture.

Moreover, if an entity, called the *requester*, requires access to a resource from another domain, the domain of the resource can authorize or deny access based on *verified* information about the requester and its device, without inherently trusting information provided by the domain of the requester, relying on a trusted third-party, or installing intrusive software on the device of the requester.

Verified information includes the identity of the requester, information on its device, and contextual information, and is produced by the requester architecture.

The resulting federated architecture is depicted in figure 3. Its components are detailed in the following sections.

A. Interoperability of Identity and Monitoring Information

The *identity* refers to an attribute, or a set of attributes, that uniquely describe an entity (or device) within a given context. Authentication is the process of establishing confidence in user identities [17].

Identity attributes (*e.g.*, country of origin, clearance level, military rank, etc.), provided by the IdM, are the basis for attribute-based access control [29]. Attributes can also represent contextual information such as geolocalization, behavior evaluation, or time of day.

FMN and MIP define standards for attributes. For example, STANAG 1059 defines country codes, and STANAG 2116 defines ranks for military personnel. Those standards are used by NATO nations to understand each other.

An alternative to standards, *e.g.*, if a specific standard does not exist, is to create agreements between members in the federation, similar to the identity mappings proposed by [25].

B. Root-of-trust Establishment

In a zero trust architecture, trust is established between entities, devices, and the architecture when entities and de-

vices are on-boarded. The root-of-trust in this relationship is implementation dependent. Examples of root-of-trust include a secret key linked to a certificate uploaded on a device, a password given to a user, or a secret shared between the device of a user and the IdM for multi-factor authentication.

Moreover, there is necessarily trust in the supply chain, as the hardware used is not always created or managed by the organization. Such trust can be based on certification, and does not exclude continuous verification.

Zero trust federation requires a similar root-of-trust, exchanged when domains are federating. For the federation framework proposed in this paper, master certificates for each domain are exchanged to authenticate information produced by each domain. Similarly to certificates and keys shared with internal entities and devices, this root-of-trust shared between domains does not imply trust. Thus, additional verifications are required to grant access to resources.

Further, a new component, called the *remote attestation verifier* (RAV), described in section II-C, is deployed in requester domains. This component is an element of trust between members of the federation: it monitors components of the requester domain responsible for authentication and context evaluation, while being managed by the resource domain, with an identity provided by the resource domain.

To ease the certification and deployment process in the requester domain, the RAV can be a component designed and implemented by the organization of the requester. The resource organization can verify its trustworthiness before federating, similarly to other supply chain components used in the architecture.

C. Attribute Verification

When a requester requests access to a resource from another domain in the federation, attributes representing the identity of the requester, its device, and the access request context are provided to the resource domain.

Those attributes are provided, and authenticated, by the requester domain.

However, there is no inherent trust between the requester and the resource domains. The root-of-trust does not guarantee trust between the domains, as components from the requester architecture can be compromised during the mission. Thus, the resource domain needs to continuously verify the integrity of the provided attributes.

1) Remote Attestation: Continuous and non-invasive verification is performed with remote attestation.

Remote ATtestation procedureS (RATS) [30] produces information on an evaluated system, the *attester*, to another remote system, the *relying party*. This information can be used by the relying party to evaluate if the attester is trustworthy [31], [32]. Remote attestation involves a component called the *verifier*, which appraises the evidence submitted by the attester [32].

Remote attestation has been evaluated by the European commission for usage in healthcare [33]. Depending on the constraints on the requester domain, remote attestation can either rely on dedicated hardware, such as a Trusted Platform Module (TPM) [34], or be software-based without requiring special hardware [35].

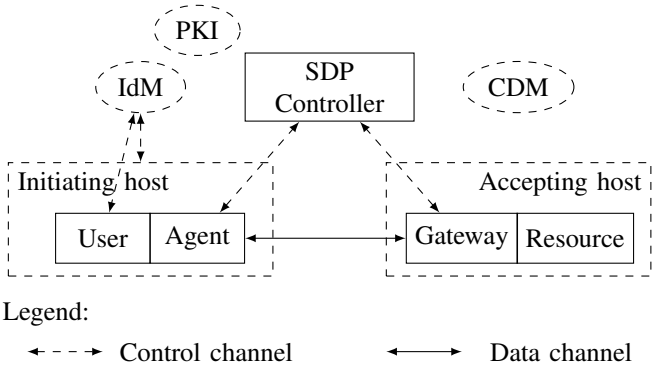


Figure 4: Architecture of SDP [37].

2) Access Requests: In the proposed federation framework, the resource architecture uses remote attestation to verify the integrity and the security posture of the IdM and CDM systems of the requester architecture. Remote attestation establishes trustworthiness in those systems, and by extension in the produced attributes.

Depending on the zero trust maturity of the resource architecture, the RAV can produce either a boolean value, indicating if the evaluated systems are in compliance with a security policy, or richer information, usable by the PDP for evaluating the access request.

III. An SDP-based federation

Software Defined Perimeter (SDP) is an abstract zero trust architecture which can be used for tactical networks. SDP-based solutions are recommended for agencies having many field agents who do not have continuous internet access and utilize many sensors and IoT devices [36].

Moreover, SDP is based on Software-Defined Networking (SDN), which offers advanced management features that can be used for interoperability [24], and for facilitating end-to-end interactions and the processing of resources in tactical networks [2].

A. Software Defined Perimeters [37]

SDP creates an overlay network on top of the existing network infrastructure. A central component, called the SDP Controller, oversees the network from the control plane. Users and resources authenticate to the SDP Controller, which is in charge of authorizing access to resources.

The components of an SDP architecture are depicted in figure 4. Every device contains a device agent, which is in charge of monitoring the device and of establishing connections with the SDP controller and SDP resources. The terminology for entities and devices trying to access an SDP resource is 'Initiating Host' (IH).

SDP resources are protected by a gateway, which filters every communication with the resource, and communicates

with the SDP Controller. By default, the gateway refuses any incoming connection. The gateway and the resource form an 'Accepting Host' (AH).

When a resource or device is on-boarded, its gateway or device agent creates a secure control channel to the SDP Controller. This channel is used to exchange information between the device or resource and the controller, such as user authentication, device validation, or an assessment of the resource security posture.

Given those elements, the controller grants or denies an IH access to an AH. This authorization is communicated to the device agent and to the gateway, the latter enforcing the access decision. IHs can then establish secure communication channels with AHs to access resources.

Secure communication channels in SDP are composed of two mechanisms: first single packet authorization (SPA), which ensures only pre-authorized entities can create the channel, and then mutual TLS, to create end-to-end encrypted and authenticated channels.

B. SDP Federation

This section presents how to create a federated SDP architecture from the generic zero trust federated architecture depicted in figure 3. The resulting architecture, and specific messages exchanged to establish trust between architectures, is depicted on figure 5.

On top of adding the RAV in the architecture, controllers need to be extended to perform federation operations, for establishing roots of trust, and for relaying information from controllers of other domains to IHs.

1) Root-of-trust Establishment: A root-of-trust is established between the controllers of both domains. This root-of-trust consists of the master certificate used for authentication, the address of the SDP controller, and a list of federated services, for each domain.

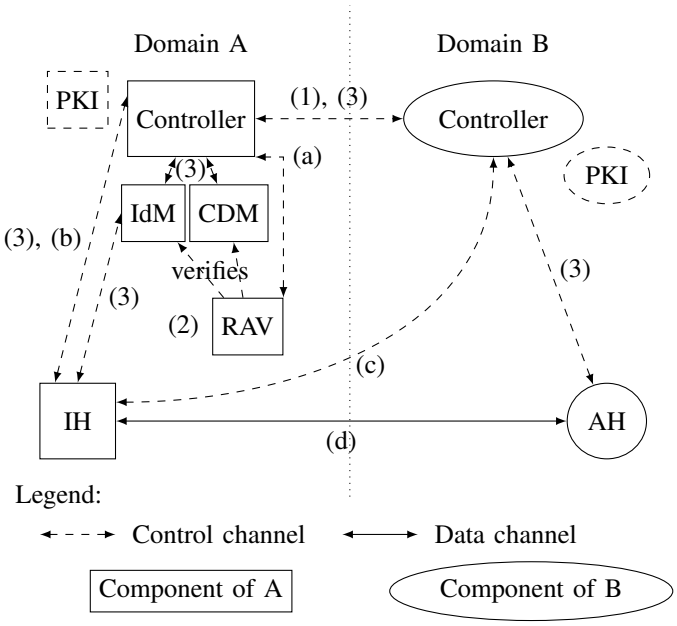
Moreover, each domain deploys a remote attestation verifier. The RAV is on-boarded, as described in section II, as a component of the resource domain deployed in the requester domain.

The RAVs continuously monitor the IdM and CDM systems of the domain in which they are deployed. This monitoring produces attributes, authenticated with keys securely stored in the RAV, with the resource domain being able to verify the authenticity of the attributes.

2) Access request: In a single SDP architecture, an IH receives, at on-boarding, a root-of-trust from its controller, as well as a list of AHs it can access.

In an SDP federation, if the IH is to access federated resources, its controller queries controllers of federation partners, with attributes describing the IH. Given those attributes, partner controllers answer with lists of AHs that the IH can access. Then, the IH receives the list of all AHs it can access, federated or not.

To access a federated resource, an IH first queries its own controller to retrieve monitoring attributes, signed by the RAV. Those attributes are then included in the access request to the AH, alongside authentication and monitoring attributes for the IH.



Federation establishment:

1) Root-of-trust establishment.
2) RAV deployment, and continuous monitoring of the integrity of the IdM and the CDM.
3) Exchange of root-of-trust and information for couples IH-AH.

Access request:

a) RAV verification attributes.
b) The IH retrieves the RAV attributes from its controller.
c) IH access request forwarded to domain B controller.
d) Secure end-to-end channel establishment.

Figure 5: Federated SDP architecture.

Upon reception of the query, the gateway of the AH forwards it to its controller, which evaluates the query and takes an access decision. The decision is then enforced by the gateway. As such, the IH from the requester domain does not communicate directly with the controller of the resource domain. There is, however, a logical communication going through the gateway, displayed in figure 5.

Once the access is granted, the IH creates a secure connection with the AH, based on SPA and mTLS.

IV. Conclusion

The operational needs for sharing of data and services between nations and domains in a coalition require interoperable federated architectures. Data and services in those architectures need to be protected against unauthorized access. This is enabled by zero trust architectures, which segment access to resources and always verify access, following strict least-privileged policies. However, state-of-the-art zero trust federation solutions either require intrusive software to be

installed on every requester device, or assume inherent trust between federation partners.

This paper has proposed a novel method to enforce the verification of every access request, even if the requester belongs to a federated partner, without assuming trust in partners. This solution is based on remote attestation, which continuously verifies the integrity and authenticity of attributes produced by federated partners. Thus, every access request is verified directly by the resource domain, which preserves the zero trust guarantees of the architecture.

This abstract novel architecture has been illustrated by an SDP-based zero trust federation.

REFERENCES

[1] N. Suri, A. Hansson, J. Nilsson, P. Lubkowski, K. Marcus, M. Hauge, K. Lee, B. Buchin, L. Misirhoglu, and M. Peuhkuri, "A realistic military scenario and emulation environment for experimenting with tactical communications and heterogeneous networks," in *2016 International Conference on Military Communications and Information Systems (ICMCIS)*. IEEE, May 2016.

[2] R. Mahmud, A. N. Toosi, M. A. Rodriguez, S. C. Madanapalli, V. Sivaraman, L. Sciacca, C. Sioutis, and R. Buyya, "Software-defined multi-domain tactical networks: Foundations and future directions," in *Mobile Edge Computing*. Springer International Publishing, 2021, pp. 183–227.

[3] J. Stoltenberg, "The secretary general's annual report 2014," 2014. [Online]. Available: https://www.nato.int/cps/en/natohq/opinions_116854.htm

[4] NATO, "Federated mission networking." [Online]. Available: https://dnbl.ncia.nato.int/FMNPublic/SitePages/Home.aspx

[5] M. R. Brannsten, F. T. Johnsen, T. H. Bloebaum, and K. Lund, "Toward federated mission networking in the tactical domain," *IEEE Communications Magazine*, vol. 53, no. 10, pp. 52–58, Oct. 2015.

[6] W. B. King, "Army europe highlights interoperability at communications conference," *U.S. Army*, 2016. [Online]. Available: https://www.army.mil/article/161837/

[7] NATO, "Multi-domain operations: Enabling NATO to out-pace and out-think its adversaries," Jul. 2022. [Online]. Available: https://www.act.nato.int/articles/multi-domain-operations-out-pacing-and-out-thinking-nato-adversaries

[8] P. Simmonds, "De-perimeterisation," 2004. [Online]. Available: https://www.blackhat.com/presentations/bh-usa-04/bh-us-04-simmonds.pdf

[9] J. Kindervag, "No more chewy centers: Introducing the zero trust model of information security," Forrester, Tech. Rep., 2010. [Online]. Available: https://media.paloaltonetworks.com/documents/Forrester-No-More-Chewy-Centers.pdf

[10] J. G. Grimes, "Vision for a net-centric, service-oriented dod enterprise," Department of Defense Global Information Grid, Tech. Rep., 2007. [Online]. Available: https://www.acqnotes.com/Attachments/DoDGIGArchitecturalVision,June07.pdf

[11] J. Rundle, "Solarwinds, microsoft hacks prompt focus on zero-trust security," *The Wall Street Journal*, 2021. [Online]. Available: https://www.wsj.com/articles/solarwinds-microsoft-hacks-prompt-focus-on-zero-trust-security-11619429402

[12] J. Biden, "Improving the nation's cybersecurity," Executive order 14028, 2021. [Online]. Available: https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity

[13] S. D. Young, "Moving the U.S. government toward zero trust cybersecurity principles," Memorandum M-22-09, 2022. [Online]. Available: https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

[14] R. Freter, "Zero trust reference architecture," Department of Defense, Tech. Rep., 2022. [Online]. Available: https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v2.0(U)_Sep22.pdf

[15] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture," National Institute of Standards and Technology, Tech. Rep. 800-207, aug 2020. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-207/final

[16] CISA, "Zero trust maturity model," CISA, Tech. Rep., 2021. [Online]. Available: https://www.cisa.gov/zero-trust-maturity-model

[17] P. A. Grassi, M. E. Garcia, and J. L. Fenton, "Digital identity guidelines: revision 3," National Institute of Standards and Technology, Tech. Rep. SP 800-63-3, Feb. 2020. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-63/3/final

[18] Cybersecurity & Infrastructure Security Agency (CISA), "Continuous diagnostics and mitigation (CDM) program," 2012. [Online]. Available: https://cisa.gov/cdm

[19] S. Bhatt, P. K. Manadhata, and L. Zomlot, "The operational role of security information and event management systems," *IEEE Security & Privacy*, vol. 12, no. 5, pp. 35–41, sep 2014.

[20] K. Strandell and S. Mittal, "Risks to zero trust in a federated mission partner environment," *arXiv preprint arXiv:2211.17073*, Nov. 2022.

[21] NATO Standardization Office, "Nato interoperability standards and profiles," 2021. [Online]. Available: https://nhqc3s.hq.nato.int/Apps/Architecture/NISP/introduction.html

[22] M. I. P. (MIP), "MIP4-IES," 2021. [Online]. Available: https://www.mip4ies.com/

[23] M. Pradhan, N. Suri, C. Fuchs, T. H. Bloebaum, and M. Marks, "Toward an architecture and data model to enable interoperability between federated mission networks and IoT-enabled smart city environments," *IEEE Communications Magazine*, vol. 56, no. 10, pp. 163–169, oct 2018.

[24] S. Khan and F. K. Hussain, "Software-defined overlay network implementation and its use for interoperable mission network in military communications," in *Advanced Information Networking and Applications*. Springer International Publishing, 2022, pp. 554–565.

[25] W. R. Simpson and K. E. Foltz, "Maintaining zero trust with federation," *International Journal of Emerging Technology and Advanced Engineering*, vol. 11, no. 5, pp. 17–32, may 2021.

[26] K. Olson and E. Keller, "Federating trust," in *Proceedings of the SIGCOMM '21 Poster and Demo Sessions*. ACM, aug 2021.

[27] K. Hatakeyama, D. Kotani, and Y. Okabe, "Zero trust federation: Sharing context under user control towards zero trust in identity federation," in *2021 IEEE International Conference on Pervasive Computing and Communications Workshops and other Affiliated Events (PerCom Workshops)*, IEEE. IEEE, mar 2021, pp. 514–519.

[28] M. Hirai, D. Kotani, and Y. Okabe, "Linking contexts from distinct data sources in zero trust federation," in *Lecture Notes in Computer Science*. Springer Nature Switzerland, 2023, pp. 136–144.

[29] B. Bezawada, K. Haefner, and I. Ray, "Securing home IoT environments with attribute-based access control," in *Proceedings of the Third ACM Workshop on Attribute-Based Access Control*. ACM, mar 2018.

[30] L. Gu, X. Ding, R. H. Deng, B. Xie, and H. Mei, "Remote attestation on program execution," in *Proceedings of the 3rd ACM workshop on Scalable trusted computing*. ACM, oct 2008.

[31] G. Coker, J. Guttman, P. Loscocco, A. Herzog, J. Millen, B. O'Hanlon, J. Ramsdell, A. Segall, J. Sheehy, and B. Sniffen, "Principles of remote attestation," *International Journal of Information Security*, vol. 10, no. 2, pp. 63–81, apr 2011.

[32] H. Birkholz, D. Thaler, M. Richardson, N. Smith, and W. Pan, "Remote ATtestation procedureS (RATS) Architecture," RFC 9334, Jan. 2023. [Online]. Available: https://www.rfc-editor.org/info/rfc9334

[33] A. Vahidi and N. Paladi, "Remote attestation of workloads in itees," ASCLEPIOS, European Commission, Tech. Rep. D4.2, 2020. [Online]. Available: https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5cfd3eb3b&appId=PPGMS

[34] D. Schellekens, B. Wyseur, and B. Preneel, "Remote attestation on legacy operating systems with trusted platform modules," *Science of Computer Programming*, vol. 74, no. 1-2, pp. 13–22, dec 2008.

[35] A. Seshadri, A. Perrig, L. van Doorn, and P. Khosla, "SWATT: software-based attestation for embedded devices," in *IEEE Symposium on Security and Privacy, 2004. Proceedings. 2004*. IEEE, 2004.

[36] K. Uttecht, "Zero trust (ZT) concepts for federal government architectures," MASSACHUSETTS INST OF TECH LEXINGTON, Tech. Rep., 2020. [Online]. Available: https://apps.dtic.mil/sti/citations/AD1106904

[37] J. Garbis and J. Koilpillai, "Software-defined perimeter (SDP) specification v2.0," Cloud Security Alliance, Tech. Rep., 2022. [Online]. Available: https://cloudsecurityalliance.org/artifacts/software-defined-perimeter-zero-trust-specification-v2/