On the Zero-Trust Intranet Certification Problem

Danielle Badenhorst, Graham Barbour, André McDonald, Wian Gertenbach and Ethan Buckinjohn
Council for Scientific and Industrial Research, Pretoria, South Africa

DBadenhorst@csir.co.za
GBarbour@csir.co.za
AMcdonald@csir.co.za

Abstract: Securing corporate networks and ensuring the trustworthiness of network resources are critical security concerns for organisations in today's interconnected digital landscape. The *zero-trust security model* is an approach to designing and implementing ICT systems which prescribes that clients and servers cannot be trusted automatically, even when connected to networks traditionally considered trusted. The implementation of the zero-trust model within the corporate *intranet* requires a secure method to verify the identity of local servers. On the *Internet*, trust in the identity of public servers is established by well-known public Certificate Authorities (CAs), which issue digital certificates to securely identify servers. However, local *intranet* servers exist within the internal address space of the network. Consequently, it is impossible to naturally obtain digital certificates for these servers, validly signed by a public CA, without publicly disclosing sensitive information such as intranet server Domain Name System (DNS) records. This leaves organisations with the option of relying on endpoint management systems to install custom CA root certificates on all corporate browsers or, in some cases, ignoring the problem altogether. In this paper, we draw on practical experience in the deployment of cybersecurity devices in corporate intranets to formally define the *intranet certification problem*. We specify five requirements that a solution to this problem must satisfy. We then conduct a comprehensive review of existing candidate solutions and academic research relevant to the intranet certification problem. Specifically, existing ICT systems for public key infrastructure and endpoint management are identified and evaluated with respect to their ability to meet the stated requirements for solving the intranet certification problem, as well as their cost. Our study reveals that solutions that meet the technical and security requirements of the intranet certification problem are beyond the reach of smaller private sector companies and public sector organisations in underdeveloped and emerging economies. The high cost and technical expertise required for their implementation and management render these solutions impractical. Consequently, by relying on servers with self-signed certificates, these entities inadvertently leave their servers susceptible to impersonation, information theft, and unauthorised resource access, thus violating the fundamental principles of the zero-trust model. We conclude that a gap exists for a simple, cost-effective, and easily managed solution to the intranet certification problem.

Keywords: Zero-trust, Public-key infrastructure, Endpoint management, Man-in-the-middle, Self-signed certificates, Intranet

1. Introduction

Network perimeters have become increasingly blurred with the advent of cloud computing and the widespread use of virtual private networking. Securing corporate networks and ensuring the trustworthiness of network resources in this interconnected landscape are critical security concerns (He et al., 2022). The zero-trust security model offers a promising approach to address these challenges, advocating for continuous entity verification and strict access control (Bobbert and Scheerder, 2022).

The *zero-trust security model*, also referred to as the *zero-trust architecture*, describes an approach to the design and implementation of Information and Communication Technology (ICT) systems (Sarkar et al., 2022; Stankard, 2021). The zero-trust model assumes that there is no traditional network perimeter; networks can be located in the cloud, locally, or as a hybrid of both. Hence, the model prescribes that clients and servers cannot be trusted automatically, even if they are connected to permissioned networks that have traditionally been considered trusted environments. The zero-trust model is implemented by establishing strong identity verification, validating device compliance before granting access, and ensuring least privilege access to only explicitly authorised resources. Zero-trust prescribes a "first verify, *and then* trust" approach (Bobbert and Scheerder, 2022; He et al., 2022). This differs from perimeter-based security, which follows a "*trust and verify*" approach.

The need to implement the zero-trust security model in the corporate intranet is attributed to two factors that erode trust within these networks (Stankard, 2021):

- Modern corporate networks consist of many interconnected zones, cloud services and infrastructure, connections to remote and mobile environments, and connections to nonconventional IT, such as Internet of Things (IoT) devices. This creates greater opportunity for network access by unauthorised entities.

- Modern cyberattacks readily bypass the network boundary and technologies such as firewalls. Examples of such attacks include phishing, social engineering, and a disgruntled employee with access to the corporate intranet.

The zero-trust model is not widely implemented in practice at present. A 2023 survey by Fortinet indicated that only 23% of respondents believed that their zero-trust strategy was fully implemented, citing a lack of information on how to best select zero-trust solutions as the primary challenge (Fortinet, 2023). However, the zero-trust model is gaining recognition as an important paradigm shift in the ICT community, and its acceptance and adoption is gaining momentum in a post-pandemic world. This is due, in part, to the issuing of a presidential executive order in the United States in May 2021 (Young, 2022). The order mandates all federal agencies to adopt zero-trust, providing a timeline until autumn 2024 to do so.

Shifting from traditional security models to the zero-trust model requires significant change. Adoption of zero-trust as a framework requires buy-in at the highest corporate level, significant planning, and deployment strategising (Microsoft, 2023a). Zero-trust adoption and acceptance cannot be defined as a simple pass or fail evaluation, but rather a business and cultural transformation; this must address elements related to governance (architecture and operations), enablers (telemetry, analytics, automation, and orchestration) as well as core domains (identities, workloads, data, networks, and devices) (Mahoutchian et al., 2022).

1.1 Zero-Trust in Corporate Intranets

Implementing the zero-trust security model on the corporate intranet requires a secure means to verify the identity of local servers. On the Internet, trust in the identity of public servers is provided by well-known public Certificate Authorities (CAs). These CAs issue digital certificates that can be used to securely identify a public server (Stapleton and Epstein, 2016). However, it is not possible to naturally use these public CAs to certify servers on the corporate intranet without publicly disclosing sensitive information such as intranet server Domain Name System (DNS) records, as these servers use an internal address space.

To establish trust in the corporate intranet, network administrators are forced to develop or implement their own solutions (often around open-source software), or to rely on third-party solutions (Kerman et al., 2020). Third-party solutions such as endpoint managers can be expensive or labour-intensive to implement, and may lead to unforeseen security vulnerabilities, particularly in multi-node environments (Zeng et al., 2014). Instead, these entities often simply ignore the problem of establishing trust in their networks, thereby leaving servers vulnerable to impersonation, and creating opportunities for information theft and unauthorised access to resources.

2. The Intranet Certification Problem

A problem concerning Zero Trust and *intranet* Hypertext Transfer Protocol Secure (HTTPS) certificates was identified practically by the authors when deploying custom security devices with web interfaces into commercial intranets. Such devices typically do not have public IP addresses, nor public DNS entries. Consequently, such devices cannot naturally present HTTPS certificates that have been signed by a well-known CA without publicly disclosing DNS records that map to internal IP addresses.

The most common approach to mitigating this problem is to use a self-signed certificate (i.e., the device itself signs the certificate). The first time a browser interacts with such a device, the user will be warned that the presented certificate is not publicly signed and must accept this self-signed certificate. This creates an opportunity for a man-in-the-middle (MITM) attack (Conti et al., 2016; De La Hoz et al., 2014). The use of these self-signed certificates also decreases zero-trust metrics (Simpson, 2022).

2.1 Problem Definition

The intranet certification problem is defined as follows: “How can intranet servers offer HTTPS services without introducing additional risks, associated with self-signed certificates, to clients?”.

To qualify as a solution, we require that a candidate ICT system must satisfy all the following requirements:

***R1**: An intranet host can generate a certificate and have it signed by a CA.*

***R2**: A client browser on the intranet will verify and accept this certificate without warning.*

***R3**: The host’s certificate must not be reusable on other intranets.*

***R4**: No private intranet information, such as DNS records, is publicly disclosed.*

***R5**: Client buy-in does not require full control of client endpoints.*

Depending on the requirements of the organisation, complete control of endpoints can be considered a negative or a positive feature. More specifically, the complexity, cost, and privacy issues introduced by endpoint management may be incompatible with the organisation's stance on security.

3. Literature Review

In this section, we consider some well-known ad-hoc candidate solutions to the intranet certification problem, as well as candidate solutions proposed in the literature.

3.1 Ad-Hoc Candidate Solutions

We consider a second ad-hoc candidate solution over and above the candidate solution of using a public CA and disclosing private IP numbers on a public DNS, as discussed in Section 2.

3.1.1 Privately disclose internal IP number via private DNS

One ad-hoc solution is to have the certificate signed by a public CA, but to only publish the DNS record on an internal (private) DNS server. While this solves the problem of public disclosure of private IP numbers and intranet names, this introduces the additional complexity and security risks of hosting a private DNS server. Hosting a private DNS server is a complex undertaking and can increase the risk of DNS attacks, such as DNS tunnelling, spoofing, or cache poisoning (NIST, 2009).

3.2 Candidate Solutions in the Literature

In this section, two relevant candidate solutions from the literature are reviewed.

3.2.1 Extension of SCEP for browsers

The Simple Certificate Enrolment Protocol (SCEP) is an example of a protocol used for issuing and managing digital certificates in networks (Rutishauser et al., 2002). SCEP is typically used in conjunction with a private (internal) CA to automate the certificate enrolment process. In a typical SCEP implementation, an intranet server (typically a device) sends a certificate enrolment request to a SCEP server, which validates the request and issues a digital certificate to the intranet server. The intranet server then uses this certificate as proof of its identity.

SCEP has been instrumental in facilitating automated certificate enrolment, thereby ensuring that certificates are always up-to-date and properly configured (Young and Honore, 2016). However, Rutishauser et al. (2002) identified a limitation of the original SCEP protocol, namely its incompatibility with browsers. This incompatibility is due to unique certificate request formats and the necessity for SCEP clients to access the private key of the certificate request. A consequence of this incompatibility is an inability to automatically install the CA certificate on the browser, thereby not meeting requirement **R2** to solve the intranet certification problem.

To address the above limitation, Rutishauser et al. (2002) proposed extensions to the original SCEP protocol, thus permitting automated CA certificate installation on browsers via a Java-based plug-in. This resulted in an implementation of SCEP client as a Java-based browser plug-in for Netscape Navigator, providing a reference for evaluating the proposed SCEP enhancements. However, these extensions to SCEP were not formally adopted. Furthermore, the proposed extension implementation plug-in was designed for Netscape Navigator only, which was discontinued in 2008.

3.2.2 X.509 home networks

Highlighting the lack of robust security features in networks, Müller et al. (2009) proposed an assisted device registration and service access system for future home networks. This assistance system facilitates the enrolment and distribution of valid X.509 certificates to new devices. These certificates can be used to control network access and ensure secure data transfer, thus addressing some of the key challenges in the implementation of a zero-trust framework in corporate intranets.

The proposed solution requires a home server with a private CA for the home network (Müller et al., 2009). When a new device wishes to register on the home network, software is installed on the new device, which then interacts with the Home Server to sign a generated certificate for the device. This is a manual process in which the Home Server manager interacts with the user of the new device via a side channel to share a PIN. If successful, the Home Server signs the certificate and returns it to the client device. The client then presents the

certificate to use facilities on the home network, such as secure video streaming using Devices Profile for Web Services (DPWS).

This solution does not satisfy requirement **R2** of the intranet certification problem. While the client is authenticated to the services, the services are not authenticated to the client. As such, it does not qualify as a solution to the intranet certification problem.

4. Existing ICT Systems as Candidate Solutions

Three technologies relevant to the intranet certification problem were identified, namely public key infrastructure managers (PKIMs), endpoint managers (EMs), and unified endpoint managers (UEMs). In Sections 4.1 to 4.3, we define these technologies and identify existing ICT systems as examples of each technology.

4.1 PKI Managers

PKIMs facilitate the processes required to implement public key infrastructure (PKI), which involves the use of digital certificates, cryptographic keys, policies, and procedures to facilitate secure communication (OpenXPKI, 2023; Microsoft, 2023b). Tasks such as issuing, revoking, or renewing digital certificates, and managing root CAs or secure key repositories are typically included in PKIM software (DigiCert Inc., 2023). Three certificate enrolment protocols widely used by PKIMs are the SCEP, the Enrolment over Secure Transport (EST) protocol, and the Certificate Management Protocol (CMP).

4.1.1 Microsoft NDES

Microsoft's NDES is a role service within Microsoft Active Directory Certificate Services that offers PKI functionality (Harwood, 2023). NDES acts as a registration authority, enabling the software on routers and other network devices and servers to generate certificates and to have them signed using the SCEP or the CMP. This allows devices without domain credentials to enrol for X.509v3 certificates from an internal CA.

4.1.2 Open-Source PKI managers

The following open-source PKIMs were identified:

- The OpenXPKI Project (OpenXPKI, 2023) is an open-source PKI trust centre. It acts primarily as an online registration authority (RA) or CA to manage X.509v3 certificates. The software provides features that include hosting issuing CAs, utilising SCEP and EST gateways for certificate distribution, hosting a certificate revocation list (CRL), and providing certificate revocation capabilities.
- Dogtag Certificate System (Dewata, 2023) is an open-source CA. It is a collection of technologies that enable the deployment of PKI on a large scale, with features including certificate issuance, revocation and retrieval, CRL generation and publishing, and other functions.
- EJBCA (EJBCA, 2023) is an open-source PKI and CA software that provides functionality such as certificate issuing, management, and validation.

4.2 Endpoint Managers

EMs provide the functionality to monitor and manage multiple nodes or endpoints in a network through automation tools or scripts to increase management efficiency (Zeng et al., 2014). Typically, an EM server is set up within the organisation's network infrastructure. This server hosts software applications that allow administrators to control various aspects of endpoint devices, including software deployment, security configurations, patch management, and remote troubleshooting.

An EM typically installs lightweight agent software on each of the endpoints (Cloudflare Inc., 2023). This software acts as a communication bridge between the endpoint and the management server. It collects data, enforces security policies, and ensures that the endpoint complies with the organisation's IT policies. EMs ensure that only authenticated endpoints can access the network, thus ensuring secure network access.

EMs present functionality to install local root CA certificates on endpoints. However, EMs do not natively offer PKI functionality to generate, issue, revoke, and renew digital certificates, nor manage root CAs.

4.2.1 Microsoft Intune

Microsoft Intune is a cloud-based endpoint management solution (Microsoft, 2023c). It manages user access to organisational resources and simplifies app and device management across multiple devices. These devices include mobile devices, desktop computers, and virtual endpoints, all of which must run Intune client software.

Microsoft Intune can install root CA certificates on endpoints, but requires an existing PKIM to be in place. Specifically, it requires a private (internal) CA and on-premises PKI infrastructure that supports the SCEP or Public Key Cryptography Standards (PKCS).

4.3 Unified Endpoint Managers

Unified endpoint managers (UEMs) combine the functionality of a PKIM (management of a private CA and digital certificates) and an EM (management of endpoints) into a single system (Cloudflare Inc., 2023). These systems can manage server certificates (i.e., certificate issuing, renewal, and revocation), as well as the ability to deploy private root CA certificates onto endpoints and their browsers.

4.3.1 Microsoft Intune paired with Microsoft NDES

Microsoft Intune can naturally integrate with Microsoft NDES to provide full UEM functionality. In this configuration, NDES provides the private (internal) CA, as well as functionality for certificate management. Intune provides endpoint management functionality, as well as the ability to install private root CA certificates on client browsers.

4.3.2 Other UEMs

VMWare Workspace ONE UEM, BlackBerry UEM, and MobileIron UEM are proprietary UEMs that manage and secure endpoints (VMware, 2023a; BlackBerry, 2021; MobileIron, 2023). These devices include mobile devices, desktops, laptops, and Internet of Things (IoT) devices. These UEMs offer certificate enrolment, CA communication, and certificate generation functionality, as well as functionality for installing root certificates on endpoints and their browsers.

5. Results

In this section, the ICT systems identified and described in Section 4 are evaluated with respect to their ability to meet the stated requirements for solving the intranet certification problem, as well as their cost. *Table 1* lists the identified PKIMs, EMs, and UEMs, and indicates whether each candidate solution satisfies each of the requirements **R1** to **R5** of the intranet certification problem. The enrolment protocols used by each system, their pricing, and whether the systems are open source or proprietary are also indicated in the table.

In sections 5.1 to 5.3, we evaluate the shortcomings of PKIMs, EMs, and UEMs generally, with regards to satisfying the requirements of the intranet certification problem. The results are summarised in Section 5.4.

Table 1: Candidate solutions to the intranet certification problem

Name of Solution	Proprietary / Open-Source	Certificate enrolment protocols	Ability to install root certificates on client	PKIM	EM	R1	R2	R3[1]	R4	R5	Pricing (USD)[2]
1. MS Intune (Microsoft, 2023d)	P	SCEP, EST	Y	N	Y	N	Y	Y	Y	N	$4 per user / month (Microsoft Security, 2023)
2. MS NDES[3] (Harwood, 2023)	P	SCEP, EST	N	Y	N	Y	N	N/A	Y[4]	Y	**Perpetual licences:** MS Server Standard: $1069 MS Server Essentials: $501

[1] *If a candidate solution is unable to install root certificates on a client, requirement **R3** will not be applicable as a consequence.*

[2] *Average listed price at time of writing (December 2023).*

[3] *Microsoft NDES is a service offering of Windows Server. Windows Server 2022 has three editions, namely Datacenter, Standard and Essentials. The Datacenter edition is used for highly virtualised datacentres or cloud environments, the Standard edition for physical or minimally virtualised environments, and the Essentials edition for small businesses with up to 25 users and 50 devices (Microsoft Windows Server, 2023a, 2023b).*

[4] *Microsoft NDES can easily be misconfigured to leak intranet DNS information publicly (Heidecker, 2021).*

Name of Solution	Proprietary / Open-Source	Certificate enrolment protocols	Ability to install root certificates on client	PKIM	EM	R1	R2	R3[1]	R4	R5	Pricing (USD)[2]
											Client Access Licences (CALs)[5]: MS Server Standard: $220 per user or device(Microsoft Windows Server, 2023a, 2023b)
3. MS Intune paired with MS NDES	P	SCEP, EST	Y	Y	Y	Y	Y	Y	Y	N	$4 per user / month (Microsoft Security, 2023) + pricing for MS NDES, as indicated above
4. VMware Workspace ONE UEM (VMware, 2023a)	P	SCEP	Y	Y	Y	Y	Y	Y	Y	N	$10 per user / month (VMWare, 2023b)
5. MobileIron UEM (MobileIron, 2023)	P	SCEP	Y	Y	Y	Y	Y	Y	Y	N	$4 per user / month (MobileIron, 2023)
6. BlackBerry UEM (BlackBerry, 2021)	P	SCEP	Y	Y	Y	Y	Y	Y	Y	N	$5 per user / month (BlackBerry UK Limited, 2023)
7. OpenXPKI (OpenXPKI, 2023)	O	SCEP	N	Y	N	Y	N	N/A	Y	Y	Free
8. Dogtag Certificate System (Dewata, 2023)	O	SCEP	N	Y	N	Y	N	N/A	Y	Y	Free
9. EJBCA Community Edition (EJBCA, 2023)	O	SCEP	N	Y	N	Y	N	N/A	Y	Y	Free

5.1 PKI Managers

Candidate solutions 2 and 7 to 9 are PKIMs. Whereas such solutions provide a private (internal) CA and the functionality for servers to generate certificates and have them signed by the private CA, such solutions do not attempt to solve requirement **R2** of the intranet certification problem. This is because the client browser's installed root CA certificates are controlled by the browser or the client operating system itself. It is not the responsibility of the PKI manager to install such root certificates on a client, as PKIMs are server orientated (i.e., not client orientated).

To configure a browser to trust a certificate generated or signed by the PKIM without warning, the user would have to manually add the root certificate of the private CA to the browser's trusted root certificates store. This is a security risk, as it means that the browser will trust the certificate even if it is invalid or has been revoked. Hence, because of the failure to satisfy requirement **R2**, PKIMs cannot be considered a solution to the intranet certification problem on their own.

[5] *A Windows Server Client Access License (CAL) is a license that grants a device or user access rights to services running on a Windows Server operating system* (Microsoft Licensing, 2023).

Candidate solutions 7 to 9 are free, open-source PKIMs. However, technical support is not offered for these PKIMs, and hence their setup and management are complex. In contrast, Microsoft NDES (candidate solution 2) requires Microsoft Server, which incurs a once-off perpetual licence fee of 501 USD (Essentials Edition) or 1069 USD (Standard Edition, for businesses with more than 50 devices or 25 users) (Microsoft Windows Server, 2023b). Microsoft Server Standard Edition incurs a further CAL cost of 220 USD per user or device (Microsoft Windows Server, 2023a).

Due to the popularity and widespread deployment of Microsoft products, we address the particular security risks of candidate solution 2 (Microsoft NDES) below.

5.1.1 Microsoft NDES security risks

Microsoft's NDES infrastructure is designed specifically to provide PKI for public-facing devices (Microsoft, 2023d). In the scenario where devices are used in an *intranet* with private IP addresses and no unique DNS names, multiple issues may arise. Microsoft NDES can allow devices on the Internet or intranet to obtain certificates; this is done by publishing the NDES URL externally from the corporate network. This can be achieved by using different methods, including Azure AD Application Proxy, Microsoft's Web Application Proxy Server, or a third-party reverse proxy. Configuring NDES for Internet or intranet access involves several components and configurations, including Secure Sockets Layer (SSL) certificates, reverse proxies, and URL publication (Heidecker, 2021). This complexity poses challenges for organisations, especially those lacking in-depth expertise, and creates the risk for misconfiguration and the subsequent disclosure of private DNS information.

Furthermore, poor integration with Microsoft NDES can pose significant security risks if it is inadequately hardened or misconfigured. If a malicious actor obtains access to the NDES Enrolment Agent certificate's private key, they could potentially request a certificate valid for logging in to the Active Directory (AD) with any subject. The malicious actor could then log on as a domain administrator using the PKINIT authentication defined in RFC 4556. A compromised AD allows malicious actors to potentially gain access to the network's most vital systems and resources, or obtain administrator privileges, thereby allowing control over the entire domain (Ebad, 2022).

5.2 Endpoint Managers

Candidate solution 1, Microsoft Intune, is exclusively an EM (i.e., it does not provide PKI functionality). In the context of the intranet certification problem, EMs provide a means of installing CA certificates in client browsers. This functionality is essential to satisfy requirement **R2** of the intranet certification problem. However, as EMs mandate full control of endpoints, all EMs fail requirement **R5.** Furthermore, it is not the responsibility of EMs to provide the necessary functionality to issue and manage certificates, which implies that EMs also fail to satisfy requirement **R1**. As a result, EMs cannot be considered a solution to the intranet certification problem.

Microsoft Intune incurs a cost of 4 USD per month for each user of a device (Microsoft Security, 2023). Note that, in order to install the root CA certificate on all devices in the network, the endpoint software needs to be installed on each of these devices.

While some organisations view full control of endpoints as a positive feature, EMs can introduce unexpected security vulnerabilities into an organisation. One example of an unforeseen security vulnerability known to the authors is where intranet web application passwords become device passwords. If the password for the intranet web application is scraped, the entire device is compromised.

5.3 Unified Endpoint Managers

Candidate solutions 3 to 6 are UEMs. Since a UEM is both a PKIM and an EM, it satisfies requirements **R1** to **R4** of the intranet certification problem. However, as an EM, these UEMs fail requirement **R5.** Hence, UEMs do not solve the intranet certification problem.

Microsoft Intune paired with Microsoft NDES (candidate solution 3) will incur the cost of both products, while the remaining UEMs considered in this study (candidate solutions 4 to 6) incur costs of between 5 and 10 USD per user per month; refer to *Table 1*.

5.4 Summary

The study reveals that although the requirements **R1** to **R4** of the intranet certification problem are solved by UEMs, these solutions are expensive. More specifically, UEMs incur a monthly cost per user and / or per client device. In addition, these solutions are also complex to implement and manage. However, as noted, no EM can satisfy requirement **R5** (by definition), and hence no UEM can. Whereas full control of client endpoints may be

compatible with some organisational policies, this potentially introduces additional security vulnerabilities on the clients and privacy concerns.

None of the candidate solutions considered in this study satisfies all the requirements (**R1** to **R5**) of the intranet certification problem. Hence, none of these ICT systems solves the intranet certification problem.

6. Conclusion and Future Work

Solutions to the intranet certification problem that satisfy the relevant technical and security requirements are beyond the reach of smaller, private sector companies and organisations in the domestic public sector, due to their excessive cost and the high level of technical expertise required to implement and manage the relevant systems (Zeng et al., 2014). The analysis of candidate solutions has indicated that EMs require full control of client endpoints, which may be incompatible with company security or privacy policies, in addition to incurring high costs. Whereas PKIMs are available as open-source software, they fail to automatically add the certificate to the browser's trusted root certificates store, thereby requiring manual intervention. This introduces additional security risks and incurs additional management overhead.

UEM solutions such as Microsoft NDES (Microsoft Server) paired with Microsoft Intune can incur costs of over 1000 USD for licencing alone and require a CAL per device or user, costing approximately 200 USD per licence (Microsoft Windows Server, 2023a, 2023b). This conclusion agrees with the authors' experience that smaller private-sector companies and public-sector organisations in underdeveloped and emerging economies often simply ignore the problem of establishing trust in their networks. In doing so, these entities leave their servers vulnerable to impersonation and create opportunities for information theft and unauthorised access to resources (Stankard, 2021).

We conclude that a technological and market gap exists for a secure, cost-effective, and low-complexity solution to the intranet certification problem. A solution that simultaneously meets these criteria promises to accelerate the implementation of the zero-trust model in corporate intranets, thereby contributing towards the safeguarding of these networks. Further, such a solution has the potential to support intranet application and device developers in the ICT domain to implement trust in their networks.

References

BlackBerry, 2021. Securing connections using PKI [WWW Document]. URL https://docs.blackberry.com/content/dam/docs-blackberry-com/release-pdfs/en/blackberry-uem/12_14/administration/Using-PKI-to-secure-connections-BlackBerry-UEM-12.14-en.pdf (accessed 9.4.23).

BlackBerry UK Limited, 2023. BlackBerry Unified Endpoint Management, (UEM) - Industry Leading Security [WWW Document]. URL https://www.applytosupply.digitalmarketplace.service.gov.uk/g-cloud/services/437061688222404 (accessed 12.13.23).

Bobbert, Y., Scheerder, J., 2022. Zero Trust Validation: from Practice to Theory : An empirical research project to improve Zero Trust implementations. In: Proceedings - 2022 IEEE 29th Annual Software Technology Conference, STC 2022. Institute of Electrical and Electronics Engineers Inc., pp. 93–104.

Cloudflare Inc., 2023. What is an endpoint? [WWW Document]. URL https://www.cloudflare.com/learning/security/glossary/what-is-endpoint/ (accessed 7.24.23).

Conti, M., Dragoni, N., Lesyk, V., 2016. A Survey of Man in the Middle Attacks. IEEE Communications Surveys and Tutorials.

De La Hoz, E., Cochrane, G., Moreira-Lemus, J.M., Paez-Reyes, R., Marsa-Maestre, I., Alarcos, B., 2014. Detecting and defeating advanced man-in-the-middle attacks against TLS. In: International Conference on Cyber Conflict, CYCON.

Dewata, E., 2023. Dogtag PKI Documentation [WWW Document]. GitHub. URL https://github.com/dogtagpki/pki/wiki (accessed 9.4.23).

DigiCert Inc., 2023. What is PKI? [WWW Document]. URL https://www.digicert.com/what-is-pki#:~:text=Public%20Key%20Infrastructure%20(PKI)%20is,users%2C%20devices%2C%20or%20services. (accessed 10.20.23).

Ebad, S.A., 2022. Lessons learned from offline assessment of security-critical systems: the case of Microsoft's active directory. International Journal of System Assurance Engineering and Management 13.

EJBCA, 2023. EJBCA CA Concept Guide [WWW Document]. URL https://doc.primekey.com/ejbca/ejbca-operations/ejbca-ca-concept-guide (accessed 9.4.23).

Fortinet, 2023. The State of Zero Trust Report.

Harwood, R., 2023. What is Network Device Enrollment Service for Active Directory Certificate Services [WWW Document]. Microsoft. URL https://learn.microsoft.com/en-us/windows-server/identity/ad-cs/network-device-enrollment-service-overview (accessed 9.4.23).

He, Y., Huang, D., Chen, L., Ni, Y., Ma, X., 2022. A Survey on Zero Trust Architecture: Challenges and Future Trends. Wirel. Commun. Mob. Comput. 2022.

Heidecker, D., 2021. NDES Security Best Practices [WWW Document]. Microsoft Security, Compliance and Identity Core Infrastructure and Security Blog. URL https://techcommunity.microsoft.com/t5/core-infrastructure-and-security/ndes-security-best-practices/ba-p/2832619 (accessed 8.30.23).

Kerman, A., Borchert, O., Rose, S., Division, E., Tan, A., 2020. Implementing a Zero Trust Architecture. NIST Computer Security Resource Center.

Mahoutchian, T., McLaughlin, M., Thayres, A., Rafla, A., 2022. Zero Trust implementation for human centered cyber security [WWW Document]. Deloitte. URL https://www2.deloitte.com/us/en/blog/human-capital-blog/2022/zero-trust-adoption-for-human-centered-cyber-security.html (accessed 6.9.23).

Microsoft, 2023a. Zero Trust adoption framework overview [WWW Document]. URL https://learn.microsoft.com/en-us/security/zero-trust/adopt/zero-trust-adoption-overview#the-zero-trust-adoption-motion (accessed 6.5.23).

Microsoft, 2023b. What is Network Device Enrollment Service for Active Directory Certificate Services [WWW Document]. Microsoft. URL https://learn.microsoft.com/en-us/windows-server/identity/ad-cs/network-device-enrollment-service-overview (accessed 9.4.23).

Microsoft, 2023c. Microsoft Intune securely manages identities, manages apps, and manages devices [WWW Document]. Microsoft. URL https://learn.microsoft.com/en-us/mem/intune/fundamentals/what-is-intune (accessed 9.4.23).

Microsoft, 2023d. Configure infrastructure to support SCEP with Intune [WWW Document]. Microsoft Learn. URL https://learn.microsoft.com/en-us/mem/intune/protect/certificates-scep-configure (accessed 8.30.23).

Microsoft Licensing, 2023. Client Access Licenses and Management Licenses [WWW Document]. URL https://www.microsoft.com/en-us/licensing/product-licensing/client-access-license (accessed 12.13.23).

Microsoft Security, 2023. Discover Microsoft Intune Plans and Pricing [WWW Document]. URL https://www.microsoft.com/en-us/security/business/microsoft-intune-pricing (accessed 12.13.23).

Microsoft Windows Server, 2023a. Windows Server 2022 Remote Desktop Services CAL [WWW Document]. URL https://www.microsoft.com/en-us/d/windows-remote-desktop-server-cal-2022/dg7gmgf0d7hx/0005 (accessed 12.13.23).

Microsoft Windows Server, 2023b. Pricing and licensing for Windows Server 2022 [WWW Document]. URL https://www.microsoft.com/en-za/windows-server/pricing (accessed 12.13.23).

MobileIron, 2023. MobileIron UEM Unified Endpoint Management [WWW Document]. AppDirect. URL https://marketplace.appdirect.com/en-US/apps/263299/mobileiron-uem/editions (accessed 12.13.23).

Müller, A., Kinkelin, H., Ghai, S.K., Carle, G., 2009. An assisted device registration and service access system for future home networks. In: 2009 2nd IFIP Wireless Days, WD 2009.

NIST, 2009. Secure Domain Name System (DNS) Deployment Guide, NIST Special Publication.

OpenXPKI, 2023. Overview [WWW Document]. OpenXPKI Documentation. URL https://openxpki.readthedocs.io/en/latest/reference/configuration/introduction.html (accessed 9.4.23).

Rutishauser, U., Schäfer, A., Müller, A.F., 2002. Open reference implementation of a SCEP v2 client.

Sarkar, S., Choudhary, G., Shandilya, S.K., Hussain, A., Kim, H., 2022. Security of Zero Trust Networks in Cloud Computing: A Comparative Review. Sustainability (Switzerland).

Simpson, W.R., 2022. Zero Trust Philosophy versus Architecture.

Stankard, T., 2021. What is Zero Trust in Terms of Cybersecurity? [WWW Document]. TitanHQ. URL https://www.titanhq.com/blog/zero-trust-cybersecurity/ (accessed 9.4.23).

Stapleton, J., Epstein, W.C., 2016. Security without Obscurity, Security without Obscurity.

VMware, 2023a. Managing Devices with Workspace ONE UEM [WWW Document]. VMWare Docs. URL https://docs.vmware.com/en/VMware-Workspace-ONE-UEM/services/UEM_Managing_Devices/GUID-AWT-MANAGINGDEVICESOVERVIEW.html (accessed 10.18.23).

VMWare, 2023b. VMware Workspace ONE [WWW Document]. URL https://www.vmware.com/products/workspace-one.html#pricing (accessed 12.13.23).

Young, J., Honore, A., 2016. Simple Certificate Enrollment Protocol Overview [WWW Document]. URL https://www.cisco.com/c/en/us/support/docs/security-vpn/public-key-infrastructure-pki/116167-technote-scep-00.html (accessed 12.13.23).

Young, S.D., 2022. M-22-09 Federal Zero Trust Strategy.

Zeng, S., Adam, C., Wu, F., Guo, S., Ruan, Y., Venugopal, C., Puri, R., 2014. Managing risk in multi-node automation of endpoint management. In: IEEE/IFIP NOMS 2014 - IEEE/IFIP Network Operations and Management Symposium: Management in a Software Defined World