IEEE SA
STANDARDS
ASSOCIATION

INDUSTRY CONNECTIONS
REPORT

INDUSTRY CONNECTIONS CYBERSECURITY IN AGILE CLOUD COMPUTING

CYBERSECURITY STANDARDS FOR CLOUD ACCESS

Authored by

David Tayouri
ELTA Systems Ltd.

Snir Hassidim
Check Point

Eitan Bremler
Safe-T

Alex Smirnov
Oracle

Prof. Asaf Shabtai
Ben-Gurion University of the Negev

IEEE

TRADEMARKS AND DISCLAIMERS

IEEE believes the information in this publication is accurate as of its publication date; such information is subject to change without notice. IEEE is not responsible for any inadvertent errors.

The ideas and proposals in this specification are the respective author's views and do not represent the views of the affiliated organization.

The Institute of Electrical and Electronics Engineers, Inc. 3 Park Avenue, New York, NY 10016-5997, USA

PDF: STDVA25242 978-1-5044-8432-9

NOTICE AND DISCLAIMER OF LIABILITY CONCERNING THE USE OF IEEE SA INDUSTRY CONNECTIONS DOCUMENTS

This IEEE Standards Association (“IEEE SA”) Industry Connections publication (“Work”) is not a consensus standard document. Specifically, this document is NOT AN IEEE STANDARD. Information contained in this Work has been created by, or obtained from, sources believed to be reliable, and reviewed by members of the IEEE SA Industry Connections activity that produced this Work. IEEE and the IEEE SA Industry Connections activity members expressly disclaim all warranties (express, implied, and statutory) related to this Work, including, but not limited to, the warranties of: merchantability; fitness for a particular purpose; non-infringement; quality, accuracy, effectiveness, currency, or completeness of the Work or content within the Work. In addition, IEEE and the IEEE SA Industry Connections activity members disclaim any and all conditions relating to: results; and workmanlike effort. This IEEE SA Industry Connections document is supplied “AS IS” and “WITH ALL FAULTS.”

Although the IEEE SA Industry Connections activity members who have created this Work believe that the information and guidance given in this Work serve as an enhancement to users, all persons must rely upon their own skill and judgment when making use of it. IN NO EVENT SHALL IEEE OR IEEE SA INDUSTRY CONNECTIONS ACTIVITY MEMBERS BE LIABLE FOR ANY ERRORS OR OMISSIONS OR DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO: PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS WORK, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE AND REGARDLESS OF WHETHER SUCH DAMAGE WAS FORESEEABLE.

Further, information contained in this Work may be protected by intellectual property rights held by third parties or organizations, and the use of this information may require the user to negotiate with any such rights holders in order to legally acquire the rights to do so, and such rights holders may refuse to grant such rights. Attention is also called to the possibility that implementation of any or all of this Work may require use of subject matter covered by patent rights. By publication of this Work, no position is taken by the IEEE with respect to the existence or validity of any patent rights in connection therewith. The IEEE is not responsible for identifying patent rights for which a license may be required, or for conducting inquiries into the legal validity or scope of patents claims. Users are expressly advised that determination of the validity of any patent rights, and the risk of infringement of such rights, is entirely their own responsibility. No commitment to grant licenses under patent rights on a reasonable or non-discriminatory basis has been sought or received from any rights holder. The policies and procedures under which this document was created can be viewed at https://standards.ieee.org/about/bog/iccom/.

This Work is published with the understanding that IEEE and the IEEE SA Industry Connections activity members are supplying information through this Work, not attempting to render engineering or other professional services. If such services are required, the assistance of an appropriate professional should be sought. IEEE is not responsible for the statements and opinions advanced in this Work.

TABLE OF CONTENTS

CYBERSECURITY STANDARDS FOR CLOUD ACCESS

ABSTRACT

The enterprises' network and network security architectures are unable to effectively serve the dynamic secure access requirements of digital business. The enterprise data center is no longer the center of access requirements for users and devices. Organizations demand immediate, uninterrupted access for their users, no matter where they are located. Digital business transformation efforts, the adoption of Software as a Service (SaaS), employees working from home (especially following the COVID-19 pandemic), and emerging edge computing platforms have changed the way enterprises work. Digital business transformation requires anywhere, anytime access to applications and services—many of which are located in the cloud.

The enterprise perimeter can now be everywhere—a dynamically created, policy-based secure access service edge. Enterprises want to protect their assets from unauthorized entities, but they also want to keep business continuity by allowing trusted devices and users to access applications hosted on premises or in the cloud. To achieve this, one of the most important security layers is the secure remote access. This paper presents the cloud security standards, with emphasis on secure remote access.

1. INTRODUCTION

In previous work, the technologies relevant to remote secure access were surveyed, and it was decided that the focus should be on the following technologies (highlighted with green), which are more pertinent to secure remote access, in four layers, as presented in the FIGURE 1, FIGURE 2, FIGURE 3, and FIGURE 4.

In this paper the existing standards for selected technologies are surveyed.

FIGURE 1 Cloud Access Infrastructure—Basic Security Components

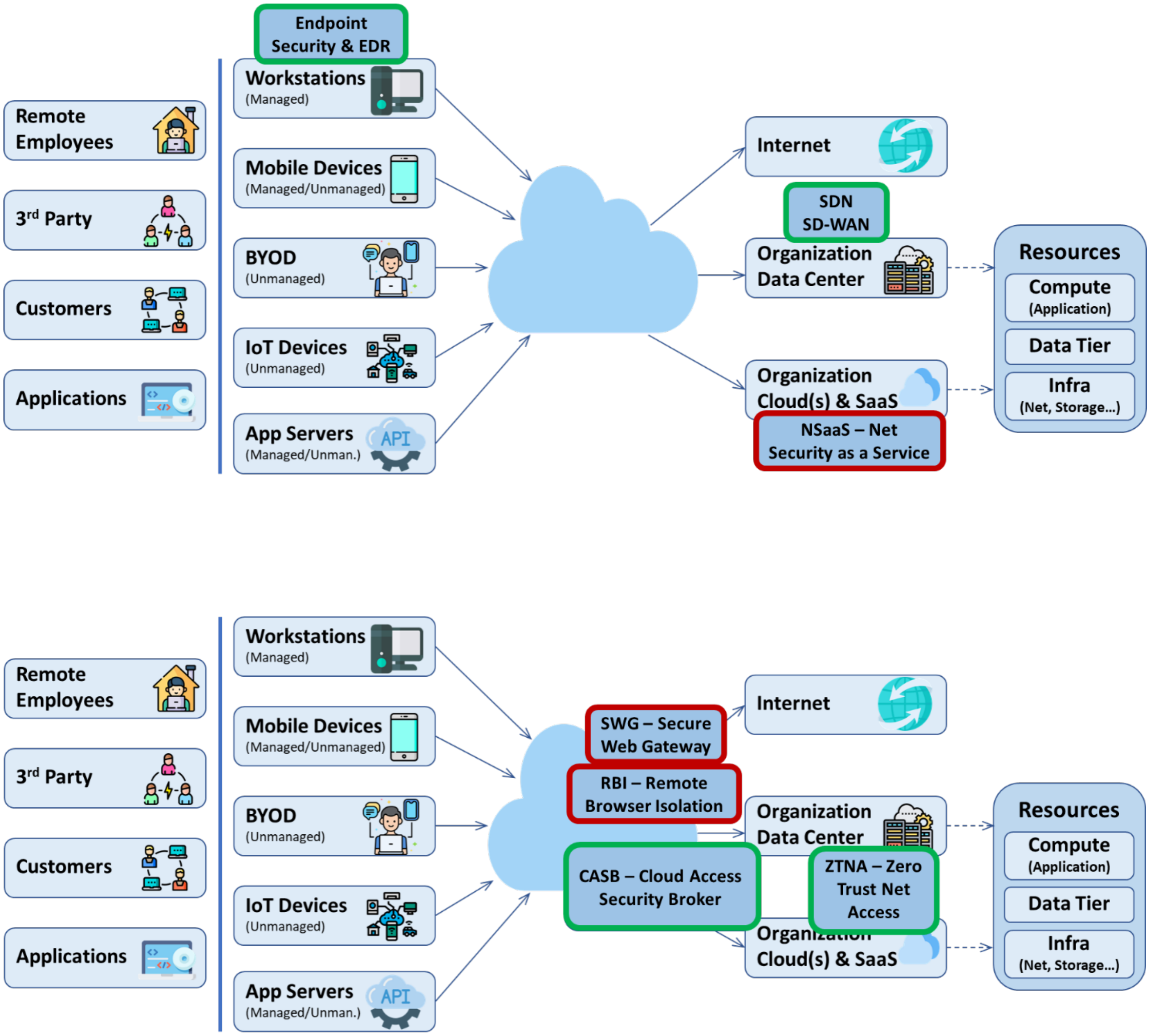
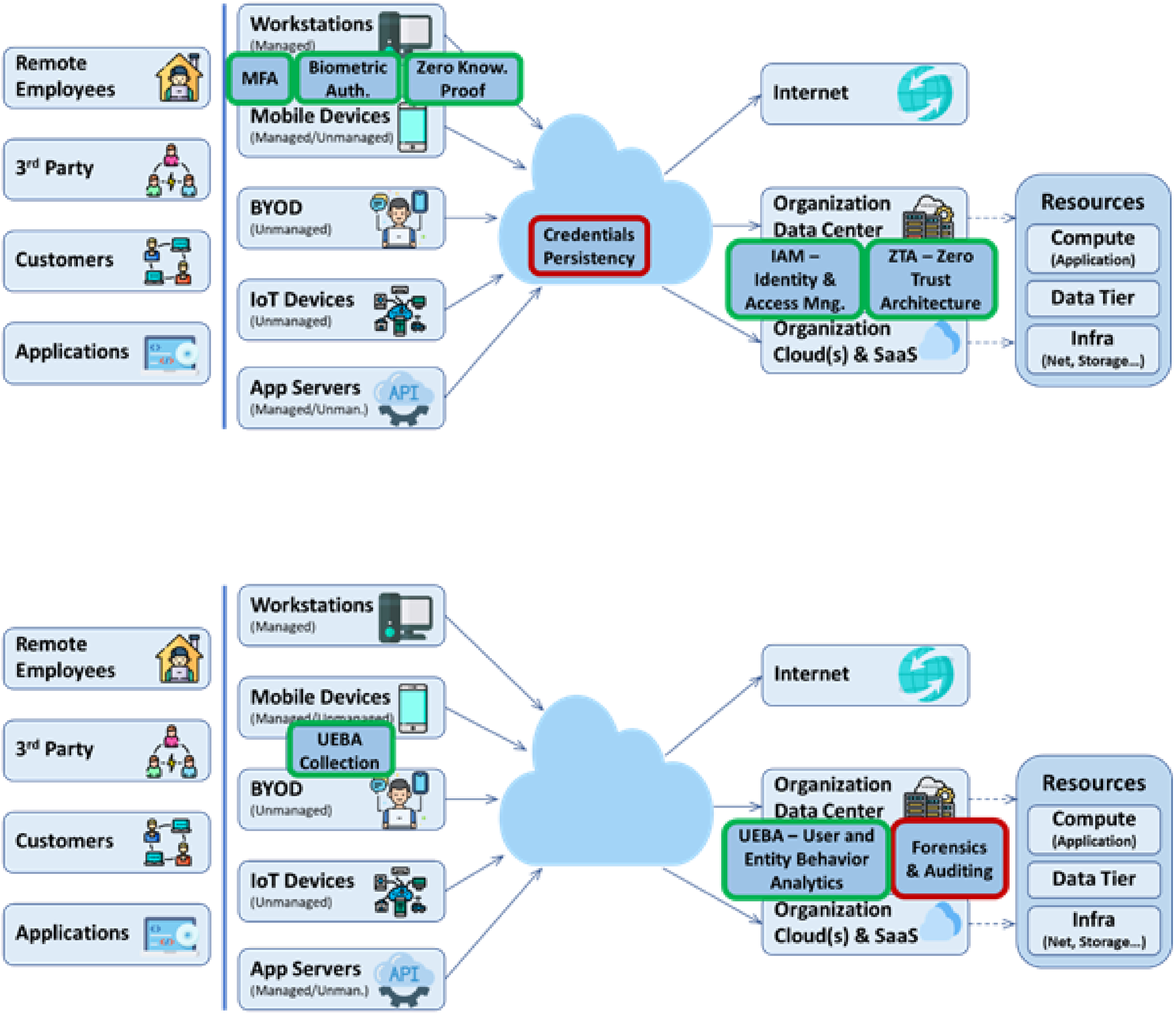


FIGURE 3 **Cloud Access Infrastructure—Identity and Authentication**



2. SOFTWARE DEFINED NETWORK (SDN) AND SD-WAN

The following standards refer to software defined network (SDN) and software defined wide area network (SD-WAN):

- IETF RFC 7426, Software-Defined Networking: Layers and Architecture Terminology [1]
    - The document describes what the layer structure is in an SDN architecture, and how layers interface with each other.
- IETF RFC 7149, Software-Defined Networking: A Perspective from within a Service Provider Environment [2]
    - The document clarifies the SDN landscape by providing a perspective on requirements, issues, and other considerations about SDN, as seen from within a service provider environment.
- MEF 70.1 SD-WAN Service Attributes and Service Framework [3]
    - The standard defines the externally-visible behavior of SD-WAN Services.
- MEF 88 Application Security for SD-WAN Services [4]
    - The standard specifies the requirements needed to add Application Flow Security to SD-WAN Services. It is based on the SD-WAN Service Attributes and Service Framework, as specified in MEF 70.1 [3], where Application Flows are comprehensively defined.
    - This standard defines Security Policy as a set of parameters, the values of which are agreed between the subscriber and service provider (as part of the SD-WAN virtual connection, SWVC, List of Policies Service Attribute) and that specify which Security Functions are to be applied to an Application Flow. It also defines Security Functions that, when enabled, enforce Security Policies on a per-Application Flow basis by performing any of the following actions: IP, port and protocol filtering, DNS protocol filtering, domain name filtering, URL filtering, malware detection and removal, or decryption and re-encryption by a middle-box function of a TLS-encrypted Application Flow. The capabilities required to support these Security Functions are also defined.

3. ENDPOINT SECURITY AND ENDPOINT DETECTION AND RESPONSE (EDR)

The following standards refer to Endpoint Security:

- NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems [5]
  - Appendix F, Section 7 describes how to implement endpoint protection platforms. This is **not** a standard for endpoint security.
- NIST SP 800-124 R2, Guidelines for Managing the Security of Mobile Devices in the Enterprise [6]
  - Section 3 describes the threats to enterprise use of mobile devices and threats to device management systems.
  - Section 4 gives an overview of mobile security technologies—device-side management and security and enterprise mobile security—and provides recommended mitigations and countermeasures.
  - Section 5 refers to enterprise mobile device deployment lifecycle.
  - This standard refers only to mobile devices, and is **not** a general standard for endpoint security.
- NC State University RUL 08.00.18, Endpoint Protection Standard [7]
  - Sections 4–5 provide guidelines for protecting university-owned endpoints and endpoints not owned by the university. These are **local** guidelines.

General standards for endpoint security were not found.

4. CLOUD ACCESS SECURITY BROKER (CASB)

Standards regarding CASB were not found.

5. USER AND ENTITY BEHAVIORAL ANALYTICS (UEBA)

Standards regarding UEBA were not found.

6. ZERO TRUST ARCHITECTURE (ZTA) AND ZERO TRUST NET ACCESS (ZTNA)

The following standards refer to Zero Trust Architecture (ZTA):

- NIST SP 800-207, Zero Trust Architecture [8]
  - Section 3 describes the logical components of ZTA.
  - Section 4 discusses the ZT deployment scenarios and use cases.
  - Section 5 describes the threats associated with ZTA.
  - Section 6 describes the ZTA and possible interactions with existing federal guidance.
  - Section 7 discusses migrating to a ZTA.
- Department of Defense (DOD) Zero Trust Reference Architecture [9]
  - Section 1 describes the strategic purposes.
  - Section 2 describes the principles.

7. MULTI-FACTOR AUTHENTICATION (MFA)

The following standards refer to Multi-Factor Authentication (MFA):

- NIST SP 800-63B, Digital Identity Guidelines, Authentication and Lifecycle Management [12]
  - Section 4 describes the authenticator assurance levels.
  - Section 5.1 describes the requirements by authenticator type, including multi-factor one-time password (OTP) devices and multi-factor cryptographic software and devices.
  - Section 10.2 describes the usability considerations by authenticator type, including the MFA types mentioned in Section 5.1.
- NIST SP 1800-17, Multifactor Authentication for E-Commerce [10]
  - Section 3.5 lists all the technologies used in the publication and provides a mapping among the generic product component term, the specific product used, the function of the product, and the NIST Cybersecurity Framework Subcategory outcomes that the product provides for the example implementations.

- Section 4 describes the architecture that was used to create the example implementations.
- Section 5 describes the solution scoping for the example implementations.
- Section 6 analyzes the security characteristics in order to understand the extent to which the publication meets its objective of demonstrating the use of MFA in an e-commerce environment.
- Section 7 presents a functional evaluation of the MFA example implementations, which were conducted to verify that they meet their objective of enabling a returning purchaser to use enhanced authentication capabilities for e-commerce transactions.
- The publication volume-C includes how-to guides.

8. IDENTITY AND ACCESS MANAGEMENT (IAM)

The following standards refer to Identity and Access Management:

- NIST SP 800-63A, Digital Identity Guidelines, Enrollment and Identity Proofing [11]
  - Section 4 describes the common pattern in which a user undergoes for identity proofing and enrollment process, whereby their identity evidence and attributes are collected, uniquely resolved to a single identity within a given population or context, then validated and verified.
  - Section 5 lists the requirements to resolve, validate, and verify an identity and any supplied identity evidence. The requirements are intended to ensure the claimed identity is the actual identity of the subject enrolling the credential service provider. In addition, the requirements are intended to ensure that scalable attacks affecting a large population of enrolled individuals require greater time and cost than the value of the resources the system is protecting.
- NIST SP 800-63B, Digital Identity Guidelines, Authentication and Lifecycle Management [12]
  - Section 4 describes three authenticator assurance levels: Low, Medium, High.
  - Section 5 provides detailed requirements for verifiers and each type of authenticator: passwords (something you know), look-up secret, out-of-band device, single/multi-factor OTP device, single/multi-factor cryptographic software/device (something you have), and biometrics (something you are).
  - Section 6 refers to authenticator lifecycle management—a number of events can affect authenticator's use: binding, loss, theft, unauthorized duplication, expiration, and revocation. This section describes the actions to be taken in response to these events.

  - Section 7 refers to session management.

- NIST SP 800-63C, Digital Identity Guidelines, Federation and Assertions [13]
  - In a federation protocol, a three-party relationship is formed between the subscriber, the identity provider, and the relying party.
  - Section 4 describes three federation assurance levels.
  - Section 5 describes federation models (manual registration, dynamic registration, federation authorities, and proxied federations), privacy requirements, and session management.
  - Section 6 refers to assertions, which are used for authentication of a subscriber, passed between identity provider and the relying party.
  - Section 7 refers to assertion presentation in a back-channel or front-channel manner from the identity provider to the relying party.
- NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations [14]
  - Section 3.1 refers to access control.
  - Section 3.7 refers to identification and authentication.
- ISO/IEC 29115, Entity Authentication Assurance [15]
  - Section 6 describes four assurance levels: Low, Medium, High, Very High.
  - Section 7 describes the actors: entity, credential service provider, registration authority, relying party, verifier, and trusted third party.
  - Section 8 provides a model for the phases and processes of entity authentication assurance: enrollment, credential management, and entity authentication.

There are several ISO/IEC standards, which are not freely available:

- ISO/IEC 24760-1/23, A Framework for Identity Management Parts 1–3
- ISO/IEC CD 29003, Identity Proofing and Verification
- ISO/IEC 29146, A Framework for Access Management
- ISO/IEC 29100, Privacy Framework
- ISO/IEC 29101, Privacy Architecture
- ISO/IEC 29134, Privacy Impact Assessment Methodology

- ISO 27002, Information Technology—Security Techniques

There are also several state-level standards, such as:

- University of Toronto, Identity and Access Management Standard [16]
- Victorian Government CIO Leadership Group, Identity and Access Management Standards [17]
- Minnesota IT Services, Identity and Access Management Standard [18]

9. BIOMETRIC AUTHENTICATION

The following standard refers to biometric authentication:

- NIST SP 800-63B, Digital Identity Guidelines, Authentication and Lifecycle Management [19]
  - Section 5.2.3 describes the limited use of biometrics for authentication.

There are several other standards that are not freely available:

- ISO/IEC 19784, Information technology—Biometric application programming interface
- ISO/IEC 19785, Information technology—Common Biometric Exchange Formats Framework
- ISO/IEC JTC 1/SC 37, Biometrics [20] lists biometric standards
- ANSI/INCITS 381, Information Technology—Finger Image Based Data Interchange Format
- ANSI/INCITS 398-2008 [R2013], Information technology—Common Biometric Exchange Formats Framework

10. ZERO KNOWLEDGE PROOF AUTHENTICATION

The following standards refer to zero knowledge proof authentication:

- IETF RFC 1704, On Internet Authentication [21]
- IETF 2945, The SRP Authentication and Key Exchange System [22]

There are several other standards that are not freely available:

- IEEE P1363.2, Draft Standard Specification for Password-Based Public-Key Cryptographic Techniques
- ISO/IEC 11770-4, Information technology—Security techniques—Key management—Part 4: Mechanisms based on weak secrets

11. ACADEMIC SURVEY OF CLOUD SECURITY

Following is a short survey of academic research in the domain of secure access standards in cloud environment.

Security Evaluation Methodology for Software Defined Network Solutions [23]—This research proposes a comprehensive methodology for organizations to evaluate security-related features available in software defined network (SDN) controllers. It suggests a structured approach to evaluate each layer of the SDN architecture (Application, Control and Data Planes). Each defined metric is matched with the security controls defined in NIST 800-53 [14].

Violations of Good Security Practices in Graphical Passwords Schemes: Enterprise Constraints on Scheme-Design [24]—This paper explores the impact of good security standards and lessons-learnt of Enterprise-level Information Security (EIS) as a model of constraint on Graphical Passwords (GPs) schemes. The paper uses standards such as NIST 800-53 [14] and the Cloud Security Association's Cloud Control Matrix to construct a subset of standards to which a new authentication mechanism, such as GPs, should conform. It then analyzes various GP schemes and shows their limitations from an EIS perspective.

Privacy by Design Architecture Composed of Identity Agents Decentralizing Control over Digital Identity [25]—This research proposes an identity architecture that satisfies the principles of privacy by design, decentralizes control over digital identity from providers to users, mitigates breach and impersonation risks, and reduces dependency on remote access passwords. The architecture is composed of interoperating identity agents that work on behalf of their owners and deploy digital identities that look and behave like identities found in one's wallet and contacts list. These identity agents strongly bind owners to their digital identities and private keys enabling them to prove who they are, protect their private data, and secure transactions. It considers NIST SP 800-63A [11] for elevating identity assurances associated with digital identities by proofing and affixing evidence to them with digital seals that cannot be repudiated.

Identifying, Authenticating and Authorizing Smart Objects and End Users to Cloud Services in Internet of Things [26]—This paper proposes a new Identity and Access Management mechanism for smart objects based on current Internet federated specifications but adapted to the specific requirements of the relevant environment. The proposed mechanism allows IoT services deployed locally or in the cloud to identify, authenticate, and authorize smart objects using HTTP and constrained application protocol (CoAP). It also allows end users to be identified, authenticated and authorized via these smart objects. It sets a level of assurance, following ISO/IEC 29115 [15], to quantify the degree of confidence in the authentication.

Taking Compliance to the Cloud—**Using ISO Standards (Tools and Techniques** [27]—This paper presents a risk-assessment approach for cloud computing software as a service (SaaS) applications derived from the ISO 27001 Information Security Management System (ISMS) standard and complemented by ISO practices for cloud security and protecting personal information in the cloud.

12. SUMMARY AND NEXT STEPS

Existing standards regarding selected cloud security technologies were reviewed, and according to the outcome, there are gaps in the following fields: Endpoint Security, CASB, and UEBA.

In the next phase, existing guidelines regarding to cloud security technologies will be reviewed, and a guide of best practices for secure remote access will be provided.

13. REFERENCES

The following sources either have been referenced within this paper or may be useful for additional reading:

[1] IETF RFC 7426, Software-Defined Networking: Layers and Architecture Terminology, https://datatracker.ietf.org/doc/html/rfc7426.

[2] IETF RFC 7149, Software-Defined Networking: A Perspective from within a Service Provider Environment, https://www.rfc-editor.org/rfc/pdfrfc/rfc7149.txt.pdf.

[3] MEF 70.1, SD-WAN Service Attributes and Service Framework, https://www.mef.net/wp-content/uploads/MEF_70.1.pdf.

[4] MEF 88, Application Security for SD-WAN Services, https://www.mef.net/wp-content/uploads/MEF_88.pdf.

[5] NIST SP 800-128, Guide for Security-Focused Configuration Management of Information Systems, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-128.pdf.

[6] NIST SP 800-124 R2, Guidelines for Managing the Security of Mobile Devices in the Enterprise, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-124r2-draft.pdf.

[7] NC State University RUL 08.00.18, Endpoint Protection Standard, https://policies.ncsu.edu/rule/rul-08-00-18/.

[8] NIST SP 800-207, Zero Trust Architecture, https://csrc.nist.gov/publications/detail/sp/800-207/final.

[9] Department of Defense (DOD) Zero Trust Reference Architecture, Prepared by the Joint Defense Information Systems Agency (DISA) and National Security Agency (NSA) Zero Trust Engineering Team, https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf.

[10] NIST SP 1800-17, Multifactor Authentication for E-Commerce, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1800-17.pdf.

[11] NIST SP 800-63A, Digital Identity Guidelines, Enrollment and Identity Proofing, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63a.pdf.

[12] NIST SP 800-63B, Digital Identity Guidelines, Authentication and Lifecycle Management, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf.

[13] NIST SP 800-63C, Digital Identity Guidelines, Federation and Assertions, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63c.pdf.

[14] NIST SP 800-53, Security and Privacy Controls for Information Systems and Organizations, https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final.

[15] ISO/IEC 29115, Entity Authentication Assurance, https://www.oasis-open.org/committees/download.php/44751/285-17Attach1.pdf.

[16] University of Toronto, Identity and Access Management Standard, https://isea.utoronto.ca/developing-standards/identity-access-management-new.

[17] Identity and Access Management Standards, https://www.vic.gov.au/identity-and-access-management-policies-and-standards.

[18] Minnesota IT Services, Identity and Access Management Standard, https://mn.gov/mnit/government/policies/security/?id=38-323904.

[19] NIST SP 800-63B, Digital Identity Guidelines, Authentication and Lifecycle Management, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63b.pdf.

[20] ISO/IEC JTC 1/SC 37, Biometrics, https://www.iso.org/committee/313770/x/catalogue.

[21] IETF RFC 1704, On Internet Authentication, https://datatracker.ietf.org/doc/html/rfc1704.

[22] IETF RFC 2945, The SRP Authentication and Key Exchange System, https://datatracker.ietf.org/doc/html/rfc2945.

[23] Nikoue, J. C., Butakov, S. and Malik, Y., Security Evaluation Methodology for Software Defined Network Solutions, 2019 International Conference on Platform Technology and Service (PlatCon), 2019, pp. 1–6, doi: 10.1109/PlatCon.2019.8669405.

[24] Vorster, J., Irwin, B. and Van Heerden, R.P. 2018. Violations of good security practices in graphical passwords schemes: Enterprise constraints on scheme-design. Proceedings of the 13th International Conference on Cyber Warfare and Security—ICCWS 2018, Washington DC, USA, 8–9 March 2018.

[25] Toth, K.C., Cavoukian, A. and Anderson-Priddy, A., 2020. Privacy by Design Architecture Composed of Identity Agents Decentralizing Control over Digital Identity. Open Identity Summit 2020.

[26] Beltrán, M., Identifying, authenticating and authorizing smart objects and end users to cloud services in Internet of Things, Computers & Security, Volume 77, 2018, Pages 595-611, ISSN 0167-4048.

[27] Weil, T., “Taking Compliance to the Cloud—Using ISO Standards (Tools and Techniques),” in IT Professional, vol. 20, no. 6, pp. 20-30, 1 Nov.-Dec. 2018, doi: 10.1109/MITP.2018.2877312.

RAISING THE WORLD'S STANDARDS

3 Park Avenue, New York, NY 10016-5997 USA http://standards.ieee.org

Tel.+1732-981-0060 Fax+1732-562-1571