Protect the Gate – Not Only Once: Continuous Access Evaluation in Practice

1st Tobias Hilbig
Munich University of Applied Sciences
Munich, Germany
0000-0002-2904-4758

2nd Vitali Serzantov
Munich University of Applied Sciences
Munich, Germany
0009-0009-3961-0416

3rd Thomas Schreck
Munich University of Applied Sciences
Munich, Germany
0000-0002-8960-6986

***Abstract*—In increasingly dynamic enterprise systems, accessing resources such as data and APIs from a static context is no longer a given. It is also common for users to access multiple services simultaneously within a session over an extended period. For example, the security posture of the accessing device may change during a session. Is the device still authorized to access specific resources in such a case? Continuous Access Evaluation addresses these and other problems related to changing context within a session. The basic principle of this technology is as follows: After each event that affects the context of access authorization, all participants in a session are informed. They then can decide on the continued authorization of access within a session for a user, an application, or a device. In this paper, we discuss the current state of this concept, ongoing standardization efforts and initial usage in large enterprise systems. Our findings indicate that the concept is well-defined and understood, resulting in rising academic interest in the topic. We assess ongoing progress in current standardization efforts, and also see notable adoption by major stakeholders.**

***Index Terms*—continuous access evaluation, authorization, zero trust architecture**

I. Introduction

In today's large enterprise environments, Single sign-on (SSO) functionality, federated authentication and authorization are ubiquitous. All major authentication and authorization systems rely on the same underlying mechanism: Upon session establishment, access is granted for a fixed duration. For that purpose, the requesting user or device receives an *Access Token* – a signed statement by an Identity and Access Management (IAM) system encoding access privileges or scopes. This token is then presented to the target system, which in turn evaluates whether the token is still valid. The circumstances under which an access token has been issued to a client might change within the predefined lifetime of the token. Be it the location, the security posture of the device, or the behaviour of the user. These factors, which are usually decisive in determining whether a user should have access to a resource, are no longer taken into account after the token has been issued – and thus represent a security risk. Issuing short-lived tokens is a common approach to mitigate this risk. While this solution can work in specific scenarios, it can reduce the usability of the system and requires repeated authentication and authorization by the user. The core problem, however, remains unsolved: In case the token is compromised, attackers gain unauthorized access to resources.

In order to improve access security, the concept of Continuous Access Evaluation (CAE) has emerged in recent years. The aim of this security technology is to continuously check whether a client is still authorized to access a resource. This allows the system to respond as quickly as possible to changes in the factors relevant to resource access. The consequences for the client's access rights then depend on the changed factors, be it the withdrawal or modification of the access scope.

In addition, CAE plays an important role in the Zero Trust Architecture (ZTA) network security model. This concept can be summarized as "Never trust, always verify". The approach is contrary to the classic perimeter-based network infrastructures and an effort to adapt to the security requirements of modern infrastructures, e.g., IoT and cloud environments, hybrid work and bring your own device (BYOD) policies. Academic interest in this approach has increased in recent years, especially with the publication of the NIST SP 800-207 standard [1]. Seven so-called "Tenets" of Zero Trust are proclaimed in this work. One of these states: "All resource authentications and authorizations are dynamic and strictly enforced before access is allowed". To conclude, both CAE and ZTA focus on continuously securing individual sessions. Taken together, CAE can prove to be an important cornerstone for the development of ZTA.

The goal of this paper to give an overview about the current state for the concept of CAE, especially with regard to existing standardization efforts and it's application in real-world systems. In addition, we propose a wide range of directions for future work. Our research question is as follows: Is CAE a concept which is implemented in the real world and what future work is necessary? The remainder of this work is structured as follows: We review related work in Section II. We then discuss the concept of CAE together with the Shared Signals Framework in Section III. Current real world usage is evaluated in Section IV. Finally, we discuss the results in Section V and propose extensive directions for future work in Section VI. The paper concludes with Section VII.

II. Related Work

Because the standardization effort for CAE is still in its early stages, academic research that picks up on it or its current implementations is still sparse. Nonetheless, there are already a few works that incorporate the subject.

Hatakeyama et al. proposed the concept of Zero Trust Federation (ZTF), which aims to apply Zero Trust Networking under identity federation [2]. They proposed a mechanism for sharing context and context updates under user control. Their implementation uses the Continuous Access Evaluation Protocol (CAEP) profile of the Shared Signals Framework (SSF). Building on this work, Hirai et al. developed a general model for context collection from various data sources [3]. Dean et al. attempted to realize a ZTA for the West Point Research and Education Network, using CAE based on Microsoft's implementation, which is the first usage in an educational and military environment [4]. In a survey, Jeong et al. recognized the CAEP profile as an effort towards actively monitoring users or devices throughout an authenticated session until its termination [5]. While this survey recognizes the CAEP, it must be noted that it primarily investigates the current use of Continuous Authentication (CA) techniques, which, opposite to CAE, focus on authentication rather than authorization.

Finally, Hourdin et al. addressed the issue of context-sensitive authorization for asynchronous communications [6]. Similar to CAE, they consider the problem of context changes after the steps of authentication and authorization have been performed. Based on an examination of static authorization, quasi-static authorization, and dynamic authorization, they propose a context-based dynamic authorization model where observers provide contextual information. Their solution also incorporates the publish-subscribe pattern.

III. Continuous Access Evaluation

The idea for a protocol for CAE was first introduced as a blog post in 2019 on the overlying topic of identity and security by Tulshibagwale [7]. It was proposed to address the challenges that arise from the growing need to authorize user sessions based on dynamic data such as IP locations, device health, and user privileges.

A. Requirements

Realizing CAE in the enterprise context ensures that authentication and authorization for users and devices is evaluated continuously within established sessions. Before discussing the concept in detail, we describe the requirements for CAE laid out in the initial proposal [7]:

1) **Publish–subscribe model:** An asynchronous communication pattern in which a publisher sends categorized messages. These messages can then be received by subscribers, which explicitly state their interest in messages of different categories.
2) **Duality:** Participants are able to act as publishers and subscribers simultaneously.
3) **Mesh network:** Multiple publishers and subscribers can work together in arbitrary constellations.
4) **Point-to-Point trust:** Participating parties must establish trust among themselves without central coordination.
5) **Security:** Communication channels between parties must ensure confidentiality, integrity and authenticity.

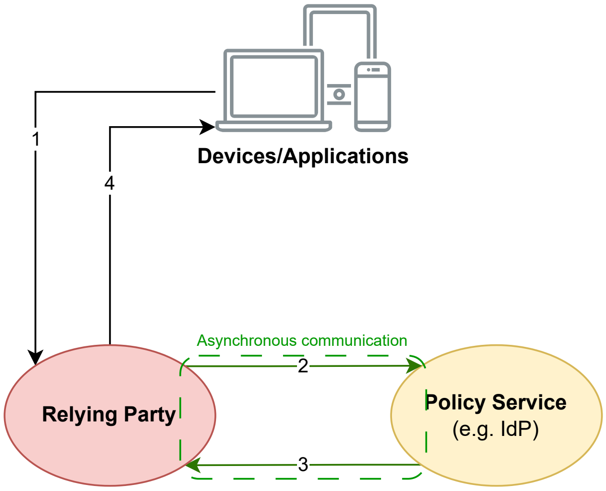

Fig. 1. The general protocol sequence of CAE [7]

6) **Selectivity:** Participants need to be able to specify the types of information they can share and receive.

B. Concept

The initial problem concerning dynamic and continuous access evaluation based on contextual data in current systems is that access authorization is only executed at the time of authentication. To solve this problem, CAE utilizes an asynchronous publish-subscribe model to enable independent parties to control the properties of user sessions. While the industry developed vendor-specific solutions to address this issue, a vendor independent, standardized protocol for this purpose could enable interoperability between security solutions and foster a common ecosystem [7], [8].

Figure 1 depicts the basic idea of CAE as an abstracted workflow diagram. The individual steps are as follows [7]:

1) **Service Request:** The device or application requests a service from a Relying Party (RP) within an authenticated user session.
2) **Context update:** If the context of the access request changed in some way from the previous access request within the authenticated session, the RP publishes this context update to all interested parties of the session. At the same time, it will be communicated if the RP is interested in receiving other updates regarding this session.
3) **User, device, or policy update:** Changes impacting a user session that are either observed or provided by other parties to the policy service, i.e., an identity provider (IdP), are processed and published to all interested parties of the session.
4) **Remediation or Response:** The response of the RP to the service request depends on the decision of the policy service. The remediation can apply to a user, device, or application. The RP's response can contain detailed information and steps to take for continued service.

C. Solution: Shared Signals Framework

The SSF, formerly known as the "Shared Signals and Event Framework" is an open standard currently developed by the Shared Signals Working Group (WG) of the OpenID Foundation, that enables asynchronous information exchange between cooperating peers [9], [10]. The SSF is developed as a Webhook Framework with a focus on security considerations. The framework is aimed to be used mainly in cross-enterprise environments [8]. In its current state, the SSF specifies two separate profiles: The Continuous Access Evaluation Protocol (CAEP) and the Risk Incident Sharing and Coordination (RISC). Both profiles are built upon the SSF core specification. The SSF is the only available realization of the CAE concept at the moment. Initially, there was only one WG for Risk Incident Sharing and Coordination (RISC), initiated by Google. After the introduction of CAE, it was recognized that similar basic requirements apply to both concepts. Therefore, both efforts were united under one WG. To understand the overall framework, it is necessary to introduce the five core concepts of the SSF first:

Events: A security-related occurrence pertaining to a Subject [11]. In practice, these events are exchanged using Security Event Tokens (SETs) [12]. SETs themselves are JSON Web Tokens (JWTs) [13] that have been specified to represent security and identity events. A JWT is a JSON object that can be signed and encrypted to securely transfer information between parties in a standardized way.

Subjects: A Subject, or Subject Principal, is an entity. Events refer to subjects and can be sent by Transmitters and received by Receivers [9]. Examples for Subjects are people, devices, groups, or organizations. Subjects are declared as JSON objects within SETs. The specification supports Simple Subjects and Complex Subjects [14]. The latter are aggregations of Simple Subjects.

Transmitter: Transmitters are entities that broadcast Events to Receivers. A Transmitter needs to implement an Event Stream Management API, a SSF specific implementation derived from the Management API for SET Event Streams [15].

Receiver: Receivers are entities that receive and act on Events. How a Receiver acts on an event is not part of the specification. To receive such Events, Receivers use the Event Stream Management API to select Subjects that they are interested in and specify how they would like to receive these Events [11].

Streams: A Stream describes the channel between Transmitters and Receivers. The SSF allows for multiple streams to exist between a Transmitter and a Receiver. The Transmitter needs to advertise whether it can push events to a Receiver, be polled for events, or both. Upon establishment of a Stream, the Receiver can choose which of the supported methods it prefers for communication.

The conceptional mode of operation of the framework can be derived from these concepts: A Transmitter is set up to transfer Events referencing different Subjects. When and on what occasions Events are triggered is not defined and is up to the Transmitter. When a Stream between a Transmitter and Receiver exists, the latter can specify which Subjects it wants to receive Events about and over which of the supported methods. API calls between Transmitters and Receivers should be secured using OAuth 2.0. Finally, Transmitters may also decide which Events to provide to a specific Receiver, as it has first to authorize itself at the Transmitter [16]. Profiles are applications of the SSF that allow exchanging certain Event types related to different use cases.

Continuous Access Evaluation Protocol (CAEP): CAEP is the first profile specified as part of the SSF and defines Event types as well as optional Event claims to ensure access security between cooperating parties [17] and addressing issues of session security [8]. It was created based on the proposal for a CAE protocol by Google [7]. In its current state, CAEP defines five Event types that relate to sessions and devices:

The *Session Revoked* Event signals the revocation of a user session. The respective session can be directly referenced or inferred via properties. A reason for the revocation can also be included in the Event. The second Event type, *Token Claims Change*, signals changes in token claims. It can encompass several claims about the specified token or assertion. At least one changed claim needs to be stated upon triggering this Event. The stated claims must only be specified with their respective new value or multiple values. Creation, revocation, update and deletion of credentials can be signaled using the *Credential Change* Event type. The specification contains ten types of credentials and additionally allows parties to agree on custom ones. Finally, the *Assurance Level Change* and *Device Compliance Change* Event types signal changes to the authentication method of the user and the device compliance status. The assurance level referred to are the Authentication and Lifecycle Management Assurance Levels defined by the NIST SP 800-63B [18]. The device compliance status can only change between *compliant* and *non compliant*.

Every type of Event can be enhanced using optional Event claims: *event_timestamp*, which specifies the exact time of an Event's occurrence, *initiating_entity*, which states the entity from which the Event originated, *reason_admin* and *reason_user*. The latter two are especially useful for giving the Receiver a human-readable context regarding a specific Event, whereas *reason_admin* is for system internal and logging purposes, and *reason_user* is addressed to the end user.

Risk Incident Sharing and Coordination (RISC): RISC, in contrast to CAEP, addresses account security. Similar to CAEP, the RISC profile defines several Event types. This includes account-related Event types that signal whether a credential change is required or an account was purged, disabled, or enabled. Identifier-related Events that reference email and phone numbers form another group. RISC also specifies Event types for opt-in and opt-out purposes. Furthermore, account recovery-related Events exist. Finally, the RISC specification contains events concerning the compromise of credentials. The *Session Revoked* Event type is deprecated in the current draft of the RISC specification [19], as this Event type was integrated into the CAEP profile.

A variety of use-cases can be handled using CAE. These use-cases can be directly derived from the respective Event types and are, at least partially, described in the specification. It is not necessary, although in theory possible, to integrate the SSF functionalities into existing authentication protocols such as OpenID Connect (OIDC) or the Security Assertion Markup Language (SAML). While the SSF recommends OAuth 2.0 for securing API calls, it works as a standalone protocol, which allows it to be used in existing enterprise systems.

IV. State of Adoption

As CAE is a fairly novel concept, there are only a few actual implementations of it. However, some of the largest corporations are among those involved in both the development and implementation of this concept.

Microsoft: The currently most prominent application of CAE is within the Microsoft Azure cloud services [20]. Microsoft announced the implementation of CAE in 2020 [21]. They employ the CAEP profile of the SSF, in which the company is also involved development-wise. It is also part of Microsoft's Azure AD Zero Trust Session Management portfolio [22]. CAE is applied to two target groups within the Microsoft Azure ecosystem: Users and workload identities. The latter are defined by Microsoft as identities used by software workloads in order to access other services or resources [23]. Examples for workload identities are containers, virtual machines, applications and services. Because CAE is allowing access decision to be taken based on different circumstances like context, location and policies, there is a need for a policy service within the ecosystem that utilizes CAE. In the case of Microsoft Azure, this service is called "Conditional Access" [24]. The current implementation of CAE for Microsoft Azure uses so-called CAE Tokens to differentiate between services with and without CAE support. Unlike conventional tokens, these do not have to rely on a static lifetime and therefore their lifetime can be as high as 28 hours [20]. The currently supported use cases include user account related changes, manual revocation, considerations of Multi Factor Authentication (MFA), risk related context changes [25], location and device state changes [26]. It is also possible to "customize" the CAE usage [27]. This means CAE can be enable or disabled for all users, individual users or specific user groups.

Google: While CAE was first proposed by Google, the CAEP profile is currently not used within the "Google Workspace". However, Google uses the RISC profile [28] for "Cross-Account Protection" features. BeyondCorp [29] is a ZTA security model developed and used by Google. It is built upon the core assumption that privileged access in a corporate network should be dependent on user and device credentials, regardless of the network location. While this model does not explicitly include CAE as a utilized technology, most of the core ideas are mentioned. It includes an access proxy component with an integrated access control engine, i.e., a policy service [29]–[31]. This access proxy authorizes services on a per-request level. Authorization decisions are based on different trust levels, taking into account various information about the user and the device. Supported authentication and authorization standards are OIDC and OAuth 2.0.

Others: Besides Microsoft and Google, Cisco is one of the better-known companies involved with CAE and the SSF. It is involved in the ongoing development of the standard within the OpenID Foundation. Cisco is also providing an initial open-source implementation of the framework as part of its Duo Lab [14]. In addition, the blog entry from Broadcom [32], as well as another open-source implementation from Sailpoint [33], indicate that the SSF and thus also CAE are attracting a certain amount of attention, especially concerning potential use in the context of ZTA. Finally, the Open Identity Exchange community utilize the SSF for fraud detection [34].

V. Discussion

In the following sections, we discuss our findings. With regard to our research question, we can conclude that CAE is indeed starting to see usage in the real world.

Concept: While Continuous Access Evaluation as a concept was only proposed recently, it is well understood and offers significant advantages to existing approaches such as restricting the lifetime of access tokens. By continuously monitoring and evaluating user behavior and access patterns, organizations can better detect and respond to potential security threats in real-time. CAE offers several benefits, including reduced threat remediation time, reduced risk of continued unauthorized access, and enhanced adaptability to evolving user and system needs.

Shared Signals Framework: The first and only standardization effort, the Shared Signals Framework, is developed by a working group at the OpenID Foundation. Two profiles have been developed, the CAEP profile for sharing status changes such as device compliance state, and the RISC profile for account security related events. The development of the standard is supported by major industry stakeholders such as Cisco, Google, Microsoft and AWS. In the last months, the draft was iteratively improved, but no more major changes were being incorporated. We therefore expect standardization to be concluded in the foreseeable future, allowing providers of IAM systems and enterprise applications to integrate it into their products.

Adoption: Since the CAE concept has not existed for very long and its standardization is still under development, it is not surprising that this technology is used in a relatively limited way. Google and Microsoft are the largest names in this regard and are already using it in production systems today. While the SSF standard specifies a set of events to be transmitted, open questions with regard to the exact use-cases exist. This might hinder the adoption, although we expect concrete use-cases to become evident with rising popularity and adoption.

Finally, the adoption by Microsoft as part of Azure indicates potential for high scalability of the concept. However, there is no data regarding the required implementation effort. It is therefore difficult to say how well it really scales with the complexity of a system. To conclude, it is unclear if smaller enterprises have sufficient resources to realize and benefit from this concept.

VI. Future Research Directions

The second part of our research question relates to necessary future work within the CAE context. In the following, we formulate detailed ideas and directions to that end.

Security, privacy and usability: The SSF specification states that all data exchange between parties must ensure standard security properties for modern protocols, i.e., confidentiality, integrity and authenticity. The broader security implementations of sharing vast amounts of user, device and service related information between a dynamic and complex set of entities are not well understood and can be the focus of future research. The usage of CAE may collide with previous assumptions about the overall system security and need to be considered carefully.

Privacy aspects are considered by the specification: The RISC profile contains events that signal a user's desire to opt-out of sharing their data with third parties. It remains to be seen if and how this opt-out process works in practice. We believe it is of great importance to ensure that user-related data, especially data that can be used to identify individuals, is only shared among parties trusted by both the service and the user. Regulatory aspects are another angle warranting further investigation, as further restrictions for data exchange between regulatory domains exist.

All security technologies need to be balanced with usability. This trade-off needs to be evaluated carefully, as "too much" security can backfire, e.g., by employees circumventing restrictions to work efficiently. The goal of CAE is to improve the security of enterprise systems without affecting usability, or even improving it. Therefore, CAE is in a unique position here. Whether this promise can hold, depends on the specific implementation and can be studied as part of future research.

Interoperability, integration and use-cases: The interoperability of CAE solutions is of great importance, since the full range of benefits can only be achieved if different systems collaborate seamlessly. The standardization of the SSF with the inclusion of necessary event types for common use-cases plays an important role here. While the standard is flexible and allows custom event types to be used, diverging implementations can hinder coordination between parties. Existing vendor-specific solutions need to be replaced or adapted to prevent the emergence of redundant, incompatible solutions. How to migrate these solutions while ensuring feature parity can be researched in the future.

Both SSF profiles do not cover all the necessary use cases. In general, use-cases are sparsely covered in the standard and need to be derived from the respective profile specifications. The use-cases are evident for some event type such as *session-revoked* but only indicated for others. Toward a broader acceptance of this standard, it will be helpful to clearly define and describe intended use cases for the SSF and its profiles. This effort can be pursued either as part of the working group at OpenID, or as "lessons-learned" during implementation in real world systems.

Performance and filtering: In large systems, one can expect thousands of events to be shared per second. Once CAE implementations are mature enough, propagation time will be a factor that needs to be investigated, as CAE's goals can only be achieved if remediation can be done promptly.

The filtering and optimization of messages that are sent within the CAE context should also be a significant subject of further research, since only a small subset of all events might be relevant to a specific party. The use of machine learning is also conceivable and could be a decisive factor with regard to the competitiveness of different CAE solutions in the industry [35].

Compatibility: CAE as a concept, and the SSF as the first standardization, are in principle independent of the underlying authentication and authorization standard. CAE had no influence on the development of the SAML, OIDC or OAuth 2.0, as the concept did not even exist in the form discussed today when these standards were developed. It also seems that CAE is not influencing the development of Grant Negotiation and Authorization Protocol (GNAP), an emerging authorization standard. Examining the integration of CAE functionalities in future authentication and authorization protocols can be a viable direction for future work.

With regard to compatibility with existing authentication and authorization standards, OIDC and GNAP are equally suitable, as both standards are based on access tokens. Contrary to that, SAML works with assertions that are consumed by an RP and are not designed to be used beyond a single session. Since these standards are designed to be extended, adapting them to support CAE functionalities is nevertheless possible.

Adoption: The adoption of CAE in general, and the SSF specifically, can be evaluated in the future. An examination of existing and emerging implementations can shed light on differences in performance, supported events and security properties. The study or development of new use-cases that might emerge with progressing adoption can also be an interesting field. As it usually is the case with emerging protocols, the adoption increases after standardization concludes. We therefore expect adoption to rise in the foreseeable future in both large and medium sized enterprises.

Zero Trust Architecture: Finally, the integration of CAE within ZTA is an apparent field of future research. One of the core ideas in ZTA is that authorization is evaluated continuously, with access being promoted, demoted or revoked on-demand. Incorporating protocols such as the SSF into ZTA solutions and products should be the next logical step.

VII. Conclusion

Continuous Access Evaluation is a concept that can be used to mitigate some of the problems we face with authentication and authorization today. Instead of making authorization decisions once at session establishment, the context of both user and device are continuously monitored, resulting in on-demand demotion, extension or revocation of access privileges. The

Shared Signals Framework, an emerging standard for CAE, can pave the way towards improving security in complex enterprise systems. Usage of the standard saw considerable uptake recently, primarily by large providers such as Microsoft and Google. We formulate multiple directions for future work in this context, focusing on privacy, interoperability and compatibility.

References

[1] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero Trust Architecture," National Institute of Standards and Technology, US Department of Commerce, Tech. Rep., Aug. 2020.

[2] 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)*, 2021, pp. 514–519.

[3] M. Hirai, D. Kotani, and Y. Okabe, "Linking Contexts from Distinct Data Sources in Zero Trust Federation," in *Emerging Technologies for Authorization and Authentication*, A. Saracino and P. Mori, Eds. Cham: Springer Nature Switzerland, 2023, pp. 136–144.

[4] E. Dean, S. Fonyi, C. Morrell, M. Lanham, and E. Teague, "Toward a Zero Trust Architecture Implementation in a University Environment," *The Cyber Defense Review*, vol. 6, no. 4, pp. 37–48, 2021. [Online]. Available: https://www.jstor.org/stable/48631305

[5] J. J. Jeong, Y. Zolotavkin, and R. Doss, "Examining the Current Status and Emerging Trends in Continuous Authentication Technologies through Citation Network Analysis," *ACM Comput. Surv.*, vol. 55, no. 6, Dec. 2022. [Online]. Available: https://doi.org/10.1145/3533705

[6] V. Hourdin, J.-Y. Tigli, S. Lavirotte, G. Rey, and M. Riveill, "Context-sensitive authorization for asynchronous communications," in *2009 International Conference for Internet Technology and Secured Transactions, (ICITST)*, 2009, pp. 1–7.

[7] A. Tulshibagwale, "Re-thinking federated identity with the Continuous Access Evaluation Protocol." [Online]. Available: https://cloud.google.com/blog/products/identity-security/re-thinking-federated-identity-with-the-continuous-access-evaluation-protocol

[8] A. Ali, M. Kiser, and A. Tulshibagwale, "A Guide to Securing Cloud Access with CAEP." [Online]. Available: https://www.idsalliance.org/webinar/a-guide-to-securing-cloud-access-with-caep/

[9] A. Tulshibagwale, "OpenID Shared Signals and Events Framework Specification 1.0 - draft 01," Jun. 2021. [Online]. Available: https://openid.net/specs/openid-sse-framework-1_0-ID1.html

[10] OpenID Foundation, "Shared Signals – A Secure Webhooks Framework | OpenID," Apr. 2015. [Online]. Available: https://openid.net/wg/sharedsignals/

[11] Shayne, Josh, CJ, Ted, and Emily, "Guide to Shared Signals." [Online]. Available: https://sharedsignals.guide

[12] P. Hunt, M. Jones, W. Denniss, and M. Ansari, "Security Event Token (SET)," Internet Requests for Comments, RFC Editor, RFC 8417, July 2018.

[13] M. Jones, J. Bradley, and N. Sakimura, "JSON Web Token (JWT)," Internet Requests for Comments, RFC Editor, RFC 7519, May 2015.

[14] Duo Labs. (2021) duolabs/sharedsignals: Python tools for using OpenID's Shared Signals Framework (including CAEP). [Online]. Available: https://github.com/duo-labs/sharedsignals

[15] M. Scurtescu and A. Backman, "Management API for SET Event Streams," Working Draft, IETF Secretariat, Internet-Draft draft-scurtescu-secevent-event-stream-mgmt-api-00, August 2017.

[16] A. Tulshibagwale, "Shared Signals: An Open Standard for Webhooks | OpenID," Aug. 2021. [Online]. Available: https://openid.net/2021/08/24/shared-signals-an-open-standard-for-webhooks/

[17] T. Cappalli and A. Tulshibagwale. (2021, Aug.) OpenID Continuous Access Evaluation Profile 1.0. [Online]. Available: https://openid.net/specs/openid-caep-specification-1_0.html

[18] P. Grassi, E. Newton, J. Fenton, R. Perlner, A. Regenscheid, W. Burr, J. Richer, N. Lefkovitz, J. Danker, Y.-Y. Choong, K. Greene, and M. Theofanos, "Digital Identity Guidelines: Authentication and Lifecycle Management," National Institute of Standards and Technology, Tech. Rep. NIST Special Publication (SP) 800-63B, Mar. 2020. [Online]. Available: https://csrc.nist.gov/publications/detail/sp/800-63b/final

[19] A. Tulshibagwale, M. Scurtescu, A. Backman, P. Hunt, J. Bradley, and S. Bounev. (2023, Feb.) OpenID RISC Profile Specification 1.0 - Draft 03. [Online]. Available: https://github.com/openid/sharedsignals/blob/main/openid-risc-profile-specification-1_0.txt

[20] Microsoft Corporation, "Continuous access evaluation in Azure AD - Microsoft Entra - Microsoft Learn," Feb. 2023. [Online]. Available: https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-continuous-access-evaluation

[21] A. Weinert. (2020, Apr.) Moving towards real time policy and security enforcement. Microsoft Entra (Azure AD) Blog. [Online]. Available: https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/moving-towards-real-time-policy-and-security-enforcement/ba-p/1276933

[22] A. Simons, "Continuous Access Evaluation in Azure AD is now generally available!" Microsoft Entra (Azure AD) Blog, Jan. 2022. [Online]. Available: https://techcommunity.microsoft.com/t5/microsoft-entra-azure-ad-blog/continuous-access-evaluation-in-azure-ad-is-now-generally/ba-p/2464398

[23] Microsoft Corporation, "What are workload identities?" Mar. 2023. [Online]. Available: https://learn.microsoft.com/en-us/azure/active-directory/workload-identities/workload-identities-overview

[24] ——, "What is Conditional Access in Azure Active Directory? - Microsoft Entra," Feb. 2023. [Online]. Available: https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/overview

[25] ——, "What is risk? Azure AD Identity Protection - Microsoft Entra," Feb. 2023. [Online]. Available: https://learn.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-risks

[26] F. Bader, "Continuous access evaluation - Cloudbrothers," Aug. 2022. [Online]. Available: https://cloudbrothers.info/continuous-access-evaluation/

[27] Microsoft Corporation, "Session controls in Conditional Access policy - Microsoft Entra," Mar. 2023. [Online]. Available: https://learn.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session

[28] Google LLC, "Protect user accounts with Cross-Account Protection | Authorization." [Online]. Available: https://developers.google.com/identity/protocols/risc

[29] R. Ward and B. Beyer, "BeyondCorp: A New Approach to Enterprise Security," *;login:*, vol. Vol. 39, No. 6, pp. 6–11, 2014.

[30] B. Spear, B. A. E. Beyer, L. Cittadini, and M. Saltonstall, "BeyondCorp: The Access Proxy," *Login*, 2016.

[31] B. Osborn, J. McWilliams, B. Beyer, and M. Saltonstall, "BeyondCorp: Design to Deployment at Google," *;login:*, vol. 41, pp. 28–34, 2016. [Online]. Available: https://www.usenix.org/publications/login/spring2016/osborn

[32] P. Connor, "The Next Evolution in Symantec Access Management." [Online]. Available: https://symantec-enterprise-blogs.security.com/blogs/feature-stories/next-evolution-symantec-access-management

[33] SailPoint, "sailpoint-oss/openid-sse-model: OpenID Shared Signals and Events (SSE) / Continuous Access Evaluation Protocol (CAEP) / Risk Incident Sharing and Coordination (RISC) JSON models in Java." Mar. 2023. [Online]. Available: https://github.com/sailpoint-oss/openid-sse-model

[34] N. Mothershaw, "OIX GUIDE TO SHARED SIGNALS," Aug. 2022. [Online]. Available: https://openidentityexchange.org/networks/87/item.html?id=580

[35] A. Ali, "CAEP: An Emerging Standard for Continuous Authentication and Access | Thales," Sep. 2020. [Online]. Available: https://cpl.thalesgroup.com/blog/access-management/continuous-access-evaluation-protocol-emerging-standard