Trustus AAM for Microsoft Cloud

CONTENTS

Trustus AAM for Microsoft Cloud

INTRODUCTION

Microsoft Solutions Partner

As a Microsoft Solution Partner, Trustus solves the critical friction points associated with high-assurance identity. We integrate seamlessly with Microsoft Entra ID to establish a cryptographically superior security foundation that accelerates your Zero Trust maturity.

Our Application Access Management (AAM) service is fully automated and transforms the entire process—from onboarding to deployment and management—into a seamless, high velocity operation. This structural synergy provides an easy, seamless, and frictionless user experience with the Microsoft cloud.

Core Capability

Zero Friction Access and Unphishable Secure Sessions

Trustus maximizes your Microsoft investment by providing the highest level of session security available. We establish the strongest cryptographic identity for every user, and maintain a direct, continuous cryptographic link to the application. This architectural control delivers an unbreakable, unphishable session by protecting the integrity of the user's access at all times.

Our advanced protection provides both zero friction user access and streamlined management for your teams. It helps your organization confidently maintain compliance standards with the strongest possible proof of identity and control.

Strategic Advantage

Real Time Command and Operational Value

Trustus provides security administrators with unparalleled management capabilities, ensuring continuous operational security and business continuity. Our solution grants real time operational capabilities—such as instant emergency service cutoffs and precise maintenance scheduling for Microsoft products—that safeguard business uptime.

By integrating this command layer directly into the access foundation, Trustus removes the complexity barrier that deters even experienced MSPs, helping you achieve full command and control of your cloud environment and maximize your security investment.

Commitment to the Customer

Trustus and Microsoft share a joint commitment to fortifying the future of enterprise cloud security. As a trusted partner, Trustus continues to align its research and development efforts with the evolution of the Microsoft Identity Platform, ensuring our customers can always rely on an integrated, forward looking security solution that grows with their strategic needs.

THE PROBLEM THAT TRUSTUS SOLVES

The Critical Misunderstanding

The market frequently harbors a critical misunderstanding: that operating within Microsoft cloud services provides absolute defense against account takeovers and breaches. This misconception often results in inadequate security controls over the user-to-cloud access path.

The Reality: Microsoft's documentation, specifically the Shared Responsibility Model[1], the Shared Responsibility in the Cloud[2], and the Artificial Intelligence (AI) Shared Responsibility Model[3] clearly mandate that the customer bear the primary duty for securing user identities and access from endpoints (laptops, phones) to the cloud applications- *"responsibility [is] always retained by the customer[4]".* Failure to address this customer-side access security is the root cause of systemic vulnerability.

THE TRUSTUS SOLUTION

Why Trustus

Trustus AAM is the safest solution to connect Microsoft users to Microsoft cloud services to access M365 Copilot, Azure, and SharePoint. The Trustus AAM Certificate-Based Authentication (CBA) provides a digitally identified and phishing resistant connection between a user's device(s) and Microsoft cloud applications.

Microsoft defines its CBA as *"a phishing-resistant authentication[5]"* and that it "*eliminates the need for federated AD FS, for a simplified environment and cost reduction[6]".*

Trustus extends this approach by ensuring its CBA provides phishing resistance not only for user authentication, but also for securing the user connection to their Microsoft applications. No other authentication/access method provides such a high level of trust.

[1] Risk assessment guide for Microsoft Cloud; https://learn.microsoft.com/en-us/compliance/assurance/assurance-risk-assessment-guide
[2] Shared responsibility in the cloud; https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility
[3] AI shared responsibility model; https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility-ai
[4] Shared responsibility in the cloud; https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility
[5] What is Microsoft Entra certificate-based authentication?; https://learn.microsoft.com/en-us/entra/identity/authentication/concept-certificate-based-authentication
[6] Ibid.

TRUSTUS' VALUE TO ORGANIZATIONS

Key Benefits of Using Trustus AAM

Trustus is the secure Certificate-Based Authentication (CBA) for digital identity and user-to-application access. Unlike traditional Identity and Access providers such as Entra ID, Trustus provides native certificate-based access and does not rely on user credentials for authentication. Nor does Trustus rely on a token-based access architecture to connect users to their applications:

I. Core Mechanism and Competitive Contrast

- Trustus AAM, being a cryptographic solution, does not rely on user credentials. Additionally, it is a tokenless system for user access and connection to their applications. Trustus AAM replaces the need for passwords, SMS OTP (one-time passcode), and the Microsoft Authenticator, all of which have been compromised to date.
- Trustus uses its native Certificate Authority ("CA"), to cryptographically identify users to prevent third-party breaches (which can happen when security providers rely on third-party external CAs). This is a serious issue since Microsoft does not provide any PKI infrastructure for implementing CBA. They state in their documentation that it is up to the customer to issue their own digital certificates and it is their responsibility to manage the certificate(s) life-cycle.[7]

II. Government-Grade Security Assurance

- Trustus CA uses only NIST FIPS 140-2 certified cryptographic products in its implementation. FIPS 140-2 is the only government approved security standard in digital communications. It is approved by the U.S. Government, Government of Canada, and is used as the ENISA standard[8] for cyber security.
- Trustus AAM X.509 digital certificates are government grade instruments of digital identity. Trustus CA is built based upon the "Certificate Policy for Access Certificates for Electronic Services" guidelines issued by the U.S. General Services Administration Federal Acquisition Service.[9]
- Trustus AAM is ideally suited to be the trusted solution providing the highest level of digital identity and encryption as mandated by the NIS2 Directive.[10]

[7] What is Microsoft Entra certificate-based authentication?; https://learn.microsoft.com/en-us/entra/identity/authentication/concept-certificate-based-authentication
[8] Standards for Cyber Security; https://www.enisa.europa.eu/sites/default/files/all_files/Standarts%20for%20Cyber%20security.pdf
[9] Certificate Policy for Access Certificates for Electronic Services Version 3.2; U.S. General Services Administration Federal Acquisition Service; May 12, 2017; https://csrc.nist.gov/CSRC/media/Projects/Computer-Security-Objects-Register/documents/ACES-CP-v3-2_signed_05122017.pdf
[10] NIS2 and the requirement for X.509 certificates; https://nis2x509.com/

III. Specific Attack Mitigation & Protection

- Stolen user credentials are rendered useless and do not impact the Trustus AAM service.
- Trustus AAM prevents the use of Microsoft stolen authentication tokens. No connection is possible between a user and their Microsoft cloud application without an approved and valid Trustus AAM digital certificate.
- A Trustus AAM digitally signed and encrypted connection prevents Man-in-the-Middle (MitM), SQL injection, and cross-site (X-site) scripting (domain redirection) attacks.

IV. Operational Simplicity and Efficiency

- Trustus has automated the entire Entra ID CBA on-boarding process, making it a simple and low-friction solution, unlike any of the authentication methods offered by Microsoft.
- Trustus AAM SaaS service ensures that the user only needs the Trustus AAM certificate on their device to connect from their browser to their application server. The organization does not require any on-prem deployment. There is no client software on the user's device (laptop, phone).

CONCLUSION

Trustus AAM is a pure SaaS platform that fundamentally simplifies and automates Microsoft Entra ID Certificate-Based Authentication (CBA). By integrating a native, FIPS 140-2 certified CA, Trustus delivers government-grade security assurance. This approach eliminates the complex, multi-step hurdles of native Entra ID CBA, resulting in a solution that is effortlessly easy to deploy and easy to use for both IT teams and end-users.

CONNECT WITH US

At Trustus, our seasoned team of technology specialists has a proven track record of architecting and delivering some of the most complex infrastructure solutions for leading international enterprises. We are uniquely equipped to help your organization rapidly implement a truly Foundational Trust model through our cloud-native platform, providing immediate, secure control over your entire digital identity ecosystem.

Explore how Trustus' team can help your organization achieve superior security and operational excellence.

- **Visit:** https://trustussecurity.com/aam-ms-cloud-brief/
- **Email:** Sales@TrustusSecurity.com
- **Connect:** https://www.linkedin.com/company/trustussecurity/