IGEL

IGEL and 90Meter - Strengthening Zero Trust Secure Access for Federal and Enterprise Environments

Introduction

Security, compliance, and interoperability are critical for organizations operating in federal and enterprise environments. To meet these demands, IGEL has expanded its partnership with 90Meter, a leading USA-based smartcard software vendor, to enhance support for Zero Trust authentication and endpoint security within IGEL OS 12. This collaboration extends native support for the 90Meter PKCS#11 smart card library to now include NIPRNet, while also updating existing SIPRNet PKCS#11 support. These advancements provide a highly secure, scalable, and policy-driven authentication solution for Virtual Desktop Infrastructure (VDI) and browser-based application deployments.

Solution Overview

The IGEL + 90Meter solution delivers a Zero Trust enterprise-grade authentication framework that secures endpoints, prevents unauthorized access, and enables strong identity verification across virtual desktop environments and browsers.

Key Capabilities:

1. **Seamless Smartcard Authentication:** Integrates 90Meter's PKCS#11 library with IGEL OS for secure smartcard authentication within virtual desktop environments.

2. **Zero Trust Endpoint Security:** IGEL OS operates under a Preventative Security Model (PSM), ensuring only verified, policy-controlled devices can access virtual workspaces.

3. **Identity and Credential Access Management (ICAM):** Supports secure authentication, certificate management, and token-based access to safeguard sensitive systems.

4. **Cross-Platform Compatibility:** Supports Citrix, Horizon, and Azure Virtual Desktop (AVD), enabling secure authentication across multi-cloud and hybrid environments.

5. **Browser-Based Access:** Enables secure smartcard authentication for virtual desktops and applications via Microsoft Edge, Chromium, and Firefox.

6. **Regulatory Compliance:** Supports DoD, NIST, and FIPS security standards, ensuring compliance with government and enterprise security mandates.

IGEL Preventative Security Model (PSM) & 90Meter Integration for ICAM

The IGEL Preventative Security Model (PSM), combined with 90Meter's PKCS#11 Library, creates a multi-layered Zero Trust security framework that enhances endpoint authentication, Identity & Credential Access Management (ICAM) compliance, and smartcard security.

IGEL OS PSM: Securing Endpoints by Design

*   **Read-Only OS:** IGEL OS operates in a locked-down state, preventing malware installation and unauthorized modifications.

*   **No Local Data Storage:** Ensures authentication credentials and sensitive data remain secured within federal networks or cloud-hosted virtual desktops.

*   **Trusted Boot & Chain of Trust:** Validates the integrity of OS components at startup, preventing device tampering and unauthorized changes strengthening your Zero Trust platform.

- **Centralized Security Management:** IGEL's Universal Management Suite (UMS) enforces policy-based security controls, ensuring only authorized devices can access 90Meter-enabled VDI environments.

90Meter PKCS#11 Library: Enabling ICAM & Strong Smartcard Authentication

- **Identity & Credential Access Management (ICAM):** Specializes in authentication, certificate, and token management, supporting secure application access, cloud authentication, and data protection.

- **Two-Factor Authentication (2FA):** Supports smartcard-based identity verification for secure, policy-controlled access.

- **Enterprise-Grade PKI Support:** Fully integrates with Zero Trust federal authentication protocols, ensuring secure access across VDI and browser-based platforms.

- **Broad Compatibility:** Supports authentication for Citrix, Omnissa Horizon, Azure Virtual Desktop (AVD), and browser-based access via Microsoft Edge, Chromium, and Firefox.

Key Benefits

1. Enhanced Security & Compliance

- Prevents unauthorized access by enforcing Zero Trust smartcard-based authentication and ICAM policies.

- Meets compliance requirements for DoD, NIST, and FIPS security standards.

- Eliminates endpoint attack vectors with IGEL's Preventative Security Model (PSM).

2. Simplified Authentication & User Experience

- Seamlessly integrates with existing smartcard authentication workflows.

- Enables strong identity verification for secure access to cloud, web, and VDI applications.

- Supports both VDI and browser-based authentication, giving users flexible access options.

3. Scalability & Future-Ready Design

- Supports cloud, hybrid, and on-prem authentication models.

- Easily scales across federal and enterprise environments, supporting multi-site authentication policies.

- Future-proofed for evolving security regulations, ensuring long-term compliance.

Conclusion

The IGEL + 90Meter solution delivers a validated, policy-driven authentication framework that enhances Zero Trust endpoint security, ICAM compliance, and smartcard authentication. By integrating IGEL's Preventative Security Model (PSM) with 90Meter's PKCS#11 Library, organizations gain seamless, strong authentication for virtual desktop environments and secure browser-based access.

With IGEL OS 12 and 90Meter, organizations can achieve highly secure, scalable, and compliant smartcard authentication, ensuring federal and enterprise environments remain protected against evolving security threats.

Learn more about IGEL Preventative Security for Government

IGEL