CertiPath Professional Services

Trusted digital identities are one of the most important components for securing an organization's digital and physical assets.

In its capacity as a trust framework provider, CertiPath is uniquely positioned to help enterprise personnel and vendors better understand the role identity plays in the security and integrity of critical communications and resources. CertiPath's team of subject matter experts includes authors, inventors, and top practitioners in the emerging identity space. The team consults on products, processes, and policies for numerous high-profile commercial and government entities.

- Application development leveraging Federal Information Processing Standard 201 (FIPS 201) conformant Personal Identity Verification (PIV) credentials and PIV-Interoperable (PIV-I) credentials
- Designing and testing Enterprise Physical Access Control Systems (E-PACS) and their secure use of PIV/PIV-I/CAC/CIV credentials
- Activities leveraging CertiPath's Public Key Infrastructure (PKI) expertise, including PKI interoperability with the Federal PKI trust fabric; CertiPath operates a bridge certification authority (CA) that is cross-certified with the Federal Bridge and has supported the CA owner/operator FPKI Annual Review process for a federal client
- Performing facility assessments to measure compliance with all next generation federal physical security and identity management mandates
- Developing, deploying, reviewing, and enforcing security policies that satisfy business objectives and government regulations
- Developing security Requirement Traceability Matrixes (RTMs) that trace requirements from source documents to test documents
- Developing security architectures and conducting architecture reviews
- Conducting IT security threat, vulnerability, risk, and countermeasure operations: We identify principal threats that systems might face, categorize vulnerabilities and residual risks, perform risk and vulnerability assessments, and identify and implement countermeasures
- Conducting and supporting system and subsystem testing
- Writing and maintaining playbooks on FICAM implementation
- Performing FICAM segment architecture compliance assessments: We provide services that meet FICAM requirements, including PIV issuance, key military and commercial security guidelines, federal directives, and guidance or instructions

1900 Reston Metro Plaza, Suite 303
Reston, VA 20190
www.certipath.com
sales@certipath.com

CertiPath Products: TrustSuite™

High-Assurance Digital Identity Provisioning and Management for PACS

What if you could securely credential your employees with one or more access technology tokens, automatically provision those identities and credentials to an enterprise PACS or many standalone ones, and manage certificate validation for all the credentials you trust with one easy, integrated, high-assurance solution?

CertiPath is pleased to present TrustSuite, an integrated set of digital identity products designed to make working with high-assurance credentials remarkably simple. The solution also supports organizations that have yet to migrate to high-assurance credentials. Whether you are still using proximity cards, you have a mix of proximity and high-assurance cards, you have high-assurance cards that contain proximity coils, or your organization's credentials and PACS are now entirely high assurance, TrustSuite supports your enterprise. TrustSuite offers streamlined enrollment, identity proofing, and automated provisioning/deprovisioning of identity and credential records to PACS, enabling full lifecycle management of both identities and their credentials. Having to reassociate a renewed credential with a user's existing privileges is a thing of the past. TrustSuite supports all of this within your organization and can also support it outside your organization, within a trust community. TrustSuite is a "FICAM v2" capability with additional features, including:

- Near real-time validation of high-assurance FICAM-approved credentials
- Granular control to support highly configurable access policies and multifactor authentication requirements (e.g., PIV Card Authentication, PIV Subscriber Authentication + PIN, PIV biometric authentication) to support varying customer requirements for facility, building, floor, room, and closed-area access
- System-of-systems design to withstand network outages and system unavailability and restore features automatically as connectivity is restored
- VIP business logic to allow for priority security processing overrides

TrustSuite comprises the following component products:

TrustManager® is CertiPath's integration solution for provisioning and lifecycle management of identity records and credentials across PACS. Traditionally, this capability has been possible within a single organization. However, TrustManager, when paired with CertiPath's TrustMonitor™, supports intercommunity federated provisioning as well.

TrustManager is a FICAM v2 Physical Identity Access Manager that automatically provisions and deprovisions identity records and credential records to any or all standalone PACS, enterprise PACS, and community member PACS. The latter option is a new, advanced form of

PACS provisioning supported with the pairing of TrustManager and TrustMonitor. Intercommunity federation is useful when several disparate organizations share a trust relationship to form a community. They want to provide automated physical access rights to each other's employees and, conversely, they want to automatically update or remove that same access when appropriate.

TrustZero® is CertiPath's high-assurance credential validation solution that provides robust business logic and configurability to a PACS' response for a range of possible validation conditions. Current validation system technology suffers from "revocation blindness"; a credential revocation can take up to 36 hours to impact what happens at a door. TrustZero achieves near real-time knowledge of credentials through a sophisticated layering of status-checking techniques, which reduces this operational blind spot to minutes. TrustZero is compatible with Lenel•S2 OnGuard® and Software House C•CURE™ and can interoperate with facilities that already operate HID Global's pivCLASS® software.

TrustMonitor® is a first-of-its-kind cloud-based validation system. It is best known as a credential monitoring and intelligence platform. When deployed as part of TrustSuite, in conjunction with TrustZero, TrustMonitor performs credential validation within the context of that overall intelligence. It is available as a SaaS managed service included with TrustZero. For organizations that require more control to either validate private CA certificates, serve as a multitenant capability, or both, TrustMonitor can also be deployed in private cloud and on-prem configurations. A private instance of TrustMonitor can greatly enhance credential validation and secure credential-sharing within a community of trust.

TrustVisitor® is CertiPath's solution for high-assurance visitor management. Individuals should interact with a facility's PACS even if they are visitors. TrustVisitor determines who a visitor is, on whose authority they are there, for what purpose they are there, and if they are there at the correct time. TrustVisitor then works to evaluate what credentials a visitor possesses and if the credentials will interoperate with all the access points the visitor will traverse during their visit. If a visitor has a trustable credential, TrustVisitor will automatically provision and deprovision it. If a loaner credential needs to be supplied in accord with federal policy, TrustVisitor will do that too and will update the PACS accordingly. The platform has been designed from the ground up with a specific view toward federal compliance. TrustVisitor helps organizations and facilities achieve compliance with HSPD-12, M-19-17, and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-116, Revision 1.

Although identity proofing and credential issuance can be accomplished with any credential management system, TrustSuite is fully integrated with Intercede's **MyID® PIV.** When these solutions are deployed together, organizations can experience unified identity and credential orchestration. They only need to create the stub of an identity record in their HR process and TrustSuite, with MyID, takes care of the rest. TrustManager begins its workflows by picking up

new and modified identity records from the enterprise's identity management system. Identity records are improved through further proofing, and identity vetting can take place as is appropriate. Once credentials of whatever technology are issued, TrustManager then provisions the identity record and credential record(s) to all PACS as is appropriate for the individual with their initial access grants. When a credential is revoked or updated or when an identity record is modified for something as common as a last name change, all of this information is automatically synced back to each PACS in which the individual has access. No one ever needs to visit a PACS enrollment office again. PACS enrollment stations are a thing of the past.

IdentityManager™ This user-centric, cloud wallet-based web authentication solution supports virtually all forms of authentication currently available online, making passwords unnecessary. IdentityManager is equally well suited to support commercial and federal enterprises. For federal clients, it meets the authentication gateway requirement and the Zero Trust multi-factor authentication requirement of OMB 22-09. It provides step-up and step-down authentication and leverages TrustMonitor to provide the most robust support of PKI-based authentication in the market, be it soft-certificates, PIV, PIV-I, or CAC.

PACSMANAGER™ Real-Time Physical Access Intelligence. Fragmented PACS create risky blind spots in attendance and security. PACSMANAGER ends the chaos by aggregating near real-time access events from multiple PACS into one powerful customizable dashboard.
Core Capabilities:

- Lightweight agents that stream access events across thousands of systems
- Enterprise query engine to create instant ad-hoc reports
- Visual timelines with intelligent anomaly flagging

No more manual aggregation. No more visibility gaps. Just unified, high-assurance intelligence that strengthens compliance, slashes fraud risk, and delivers ROI from day one.