White Paper

TrustVisitor® by CertiPath: Made to Meet Federal High-Assurance Standards

Version 4.1.00

Public Key Infrastructure

Even in its early days, U.S. government use of Public Key Infrastructure (PKI) was anticipated to be "a transparent part of [our] computing infrastructure." It would consist of "web[s] of interconnected bridges, switches, and directories" that would be interoperable with each other. Over the last 10 years, this early prediction has largely been realized.

Homeland Security Presidential Directive 12 (HSPD-12)[1], issued on August 27, 2004, was the watershed moment that resulted in the delivery of PKI to every federal employee and contractor via the Personal Identity Verification (PIV) card. Under HSPD-12, agencies were mandated for the first time to implement both logical and physical access control systems that used PKI—specifically, the PKI incorporated in a PIV card.

While PKI-enabled logical access preceded the introduction of PIV, PKI-enabled physical access did not. In fact, HSPD-12/FIPS 201[2] and the subsequent release of Office of Management and Budget (OMB) Memorandum M-11-11[3] brought about an entirely new family of products and a new industry niche. It has taken the federal enterprise more than a decade to realize PKI-enabled physical access control, but it is now the only form of Physical Access Control System (PACS) authorized for federal entities to procure and install.

Significant investment in PKI-based PACS is underway. Agencies such as the General Services Administration (GSA), the Department of Defense (DoD), the Department of Homeland Security (DHS), and the Department of Health and Human Services (HHS) have completed large PACS upgrade projects. Unfortunately, in each case, a significant gap in capability and security was left unaddressed. Visitors from other agencies, the same agency, or external to the federal government continue to be issued temporary paper badges, barcoded credentials, or other facility cards that are incompatible with the new PACS. Facility managers and physical security officers readily admit that their visitor control processes undermine the value and security of their new high-assurance PACS but lament the lack of an easy way to provision PIV credentials issued by other organizations into the local PACS or provide interoperable PKI-based smart cards to visitors. This capability and security gap has been exacerbated by the lack of federal guidance on managing visitors in a PIV-enabled PACS environment.

The release of NIST SP 800-116, Revision 1[4] provided much-needed guidance on visitor management, and **CertiPath's TrustVisitor** provides the means to close this security gap once and for all. TrustVisitor delivers compliance with high-assurance standards in a manner that meets the spirit and the letter of HSPD-12, SP 800-116, Revision 1, and M-19-17[5] and conforms to the recent PACS Overlay to 800-53[6] which requires all PACS to be compliant with HSPD-12.

1 HSPD-12, Homeland Security Presidential Directive 12: Policy for a Common Identification Standard for Federal Employees and Contractors, https://www.dhs.gov/homeland-security-presidential-directive-12

2 FIPS 201-3, Personal Identity Verification (PIV) of Federal Employees and Contractors, https://csrc.nist.gov/publications/detail/fips/201/3/final

3 M-11-11, Continued Implementation of Homeland Security Presidential Directive (HSPD) 12–Policy for a Common Identification Standard for Federal Employees and Contractors, https://www.cac.mil/Portals/53/Documents/m-11-11.pdf

4 NIST SP 800-116, Revision 1, Guidelines for the Use of PIV Credentials in Facility Access, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-116r1.pdf

5 M-19-17, Enabling Mission Delivery through Improved Identity, Credential, and Access Management, https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf

6 NIST SP 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations, https://www.nist.gov/privacy-framework/nist-privacy-framework-and-cybersecurity-framework-nist-special-publication-800-53

The Last Mile

A primary focus of HSPD-12 is identifying a high-assurance method for verifying the identity of visitors and the areas they subsequently access. Accomplishing these tasks requires a PACS that has the capability to:

- Understand whether a visitor is approved to gain access to a specific location at a particular time,
- Authenticate the visitor and the pedigree of the credential being presented, regardless of the issuer, and
- For the duration of the visit, provision the credential with the appropriate access level.

The vendor community has expended significant effort over the past 15 years to bring robust, PIV-enabled PACS to market. Similarly, the federal government has invested in a testing program to ensure the conformance of these products to the myriad requirements of FIPS 201 and its supporting Special Publications. A stated goal of HSPD-12, M-11-11, and M-19-17 is cross-organizational trust: the ability of an agency's PACS to rely on a PIV credential issued by another agency. The industry delivered exactly what was asked of it, PACS that can accept credentials from multiple issuers across multiple agencies. However, little time was spent on the processes required for external credentials to become known/provisioned to a PACS. The effort to establish visitor management processes and requirements was put on hold in favor of perfecting the technical interchange between the PACS and the PIV card. Integrators installing systems have had little choice but to perpetuate older, non-compatible visitor management systems to complement the new high-assurance PACS.

NIST noticed this technical gap. Just as OMB restated the intent of HSPD-12 in M-11-11, NIST has made clear the requirements and expectations for visitor management in SP 800-116, Revision 1, which states the following in Section 6.5:

"Many approaches to temporary badges are possible. However, a smart-card based solution that leverages current infrastructure and interoperates with federal PIV card readers and their applications is recommended."

The document also provides the following technical considerations for selecting a visitor management capability:

"Factors to consider during the procurement process include:

- The [M-05-24] requirement that temporary badges be visually and electronically distinguishable from PIV cards.
- Capabilities and costs of enrollment stations, which will likely be local to the facility for best turnaround time.
- The interoperability of temporary badges with PIV readers and authentication mechanisms (especially PKI-CAK for physical access).
- The assignment of unique identifiers (FASC-N or UUID) to temporary badges, to foster interoperability with PIV readers.
- The suitability of contactless-only temporary badges for physical access.
- The performance, cost, and security tradeoffs between disposable and reusable temporary badges required for their job function."

In 2014, DoD realized that visitor management controls were necessary to help protect the agency's facilities, assets, and personnel. One of DoD's physical security policies, DTM 09-012,[7] Attachment 4, makes electronically verifiable credentials the minimum requirement for visitors to any DoD location. DTM 09-012 states that all PACS must be upgraded (as funding becomes available) to read other agencies' credentials (e.g., PIV) and states further that unescorted visitors without these credentials are to be furnished "locally produced, temporary issue, visitor identification" that interoperates with the PACS in the same electronic fashion.

7 DTM 09-012, Interim Policy Guidance for DoD Physical Access Control, https://www.hsdl.org/?abstract&did=800675

Who and When

A visitor is a person who is scheduled to meet with someone or go somewhere at a location. A person known as an "event sponsor" initiates the need for and the scope of a visit. The purpose of the visit could be to attend a meeting or maintain some part of a facility. The event sponsor knows whom they want to attend, the event purpose, and where and when the event will take place—even if it is a self-service hoteling request where the sponsor is implicitly the organization. Those details are the starting point for any visitor workflow. A visitor management system needs to:

- Create an event with a list of participants, the event time, and the location;
- Create a local identity for each visitor;
- Associate relevant identifying documents, such as possession of a PIV card or government issued ID, with each visitor; and
- Map the location from the human-recognized identity (building name, floor, and room number) to the set of PACS access grants necessary for visitors to gain access to the event location.

In the context of HSPD-12, a visitor is someone who meets either of the following criteria:

1. Does not possess a credential that can be provisioned into the PACS but is approved for access on a temporary basis.
2. Possesses a credential that can be provisioned into the PACS but the access grant expires before the credential does.

Routine Access vs. Visitor Access

A HSPD-12 compliant PACS understands a person by his or her credential number and the locations to which the person has been granted access. The duration of the access grant begins on the day and minute the grant is established and expires contemporaneously with the person's credential. This access grant duration (routine access) is appropriate for routine access personnel (e.g., employees and contractors who require regular access to a facility for 6 months or longer), but not for visitors. For visitor access, the date and time attributes of a visitor's access grant should reflect the duration of the approved stay or event timeframe (i.e., a time period and an expiration date are assigned to temporary credentials provided to visitors).

If a visitor has a credential, they will be known by the credential number. This affords an opportunity for situational awareness. Visit requests and any issues that arise during a visit can be tracked over time for any given visitor. This tracking capability becomes particularly useful when multiple facilities are correlated across a large geography.

If a visitor does not have a credential, gathering the person's email address and driver's license or passport number affords a lesser but still useful degree of identifying information to gain a similar level of situational awareness.

Some agencies require background checks to establish trustworthiness or suitability before granting access to a building. Visitors with PIVs or CACs will have established sufficient suitability for access in most cases, but visitors without either of these credentials will need a suitability check at this stage in the process.

What

Visitors are authenticated by what they possess, their credentials. Recall that the goal of high-assurance PACS is to verify a visitor by validating a credential already in the visitor's possession. As high-assurance credentials become commonplace, this will become the status quo. However, for the foreseeable future, facility owners will need to interact with several different use cases and credentials. Currently, five (5) credential use cases are associated with visitor management in the federal enterprise:

1. "Native" agency issued PIV/PIV-I/CAC (the facility is part of the same agency that issued the credential)
2. Other agency issued PIV/PIV-I/CAC
3. Non-federally issued PIV-I
4. Locally issued, personalized PIV-C (e.g.., CIV)
5. Locally issued, non-personalized credential (e.g., facility badge)

Where

To many facility owners, location may seem to be the easiest part of visitor management. In truth, it can be the most complicated aspect.

Consider the following scenario: A subagency or reserve component is situated on the campus of the parent agency or branch. A visitor is coming for a sensitive meeting at a secured room on a lower level of the subagency's or reserve component's facility. Keep in mind that the intent is for an approved visitor to use their credential to transit all access points by electronically interacting with the PACS(s). In this scenario, the visitor must be provisioned into the front gate PACS of the parent organization, the PACS operating the front door of the subagency, the PACS for the elevator, the PACS for an interior door, and finally the PACS for the secured room. To further complicate matters, it is possible or even likely that most of the access points are controlled by different PACS instances. It is also likely that more than one brand of PACS is involved.

A visitor management system must define valid visit locations at any given facility and understand which access points must be traversed to transit from the facility's ingress point to the visit location.

Why

This is the final aspect of visitor management that must be addressed. Facility/physical security officers and PACS administrators are expected to know why each person is provisioned into the PACS and why a specific access level is granted. These details are particularly important for visitors as these temporary, relatively unknown entities represent a heightened risk exposure. Unless a visitor approval workflow capability is engaged prior to provisioning a credential to the PACS, it is not possible to have a consistent and accurate source of information that explains why access was granted.

This challenge is compounded at facilities that have multiple access points which must be traversed in order to reach a visit location. In the scenario described above, it is almost certainly guaranteed that the approvers for the front gate are not the same as the approvers for the secured room, and the approvers for the in-between access points may also be different personnel.

How: Putting It All Together With TrustVisitor

CertiPath's TrustVisitor is designed to enable security officers and PACS administrators to address the Who, When, What, Where, and Why aspects of visitor management in a repeatable and automated fashion. With the TrustVisitor solution, all visit requests are administered from the same interface and all visitors interact with the same system.

TrustVisitor provides all the necessary provisioning information to the PACS (or to each of the PACS) associated with a visitor's approved access. No human interaction is required. For greatest control, personnel can be assigned as location approvers and security approvers.

TrustVisitor is a point of aggregation for all the PACS across all the facilities in an enterprise. The platform distinguishes between visitor requests by persons with approved interoperable credentials and visitor requests by persons without approved interoperable credentials.

TrustVisitor is integrated with many of the FIPS 201 Approved Product List (APL) PACS. More PACS are being added with each release.

In addition to meeting every high-assurance visitor management requirement, TrustVisitor incorporates a robust set of features that are not always supported by competing commercial or high-assurance visitor management solutions. The following chart lists just a few of TrustVisitor's distinguishing capabilities:

Key: X not supported ✓ partially supported ✓ **FULLY SUPPORTED**

Feature	Commercial Visitor Management	Typical High Assurance Visitor Management	TrustVisitor
Fully HSPD-12/FICAM compliant	X	✓	✓
Scheduled, unscheduled, and unregistered visitors	✓	✓	✓
Clientless email and calendar integration	X	X	✓
Background check integration	✓	✓	✓
Preregister a personal electric credential remotely	X	X	✓
Assign a temporary electronic visitor credential	X	✓	✓
Fully customizable event and visitor workflows, driven by User Defined Fields	X	✓	✓
Secure multi-tenant enterprise functionality	X	✓	✓
Provision tailored visitor access in facility access control system	X	✓	✓
Interoperable with multiple PACS at one facility	X	X	✓
VIP visitors	✓	✓	✓
Touchless kiosk check-in	✓	✓	✓
Employee and visitor wellness pre-screening	✓	✓	✓
Assign a temporary credential for a forgotten employee badge	X	X	✓

The TrustVisitor Experience

In a high-assurance visitor management process, the event sponsor, visitor, approver, and lobby guard play key roles. The TrustVisitor solution reimagined this process to create the absolute best possible experience for each role while adhering to the stringent security demands of a complaint system. Automation creates a user experience that differs from the antiquated manual tediousness inherent with competing solutions. Through such features as automatic event creation, fully customizable event and visitor workflow, user defined fields, email notification, background check, ID scanning, VIP privileges, unscheduled and unregistered visitor processing, and kiosk self-check in, TrustVisitor clients have found that more than 95% of the people involved in their end-to-end visitor management process can complete their tasks in a few seconds with little to no training required. The result, especially in an enterprise-wide deployment, is significant savings in time and money coupled with high adoption rates.

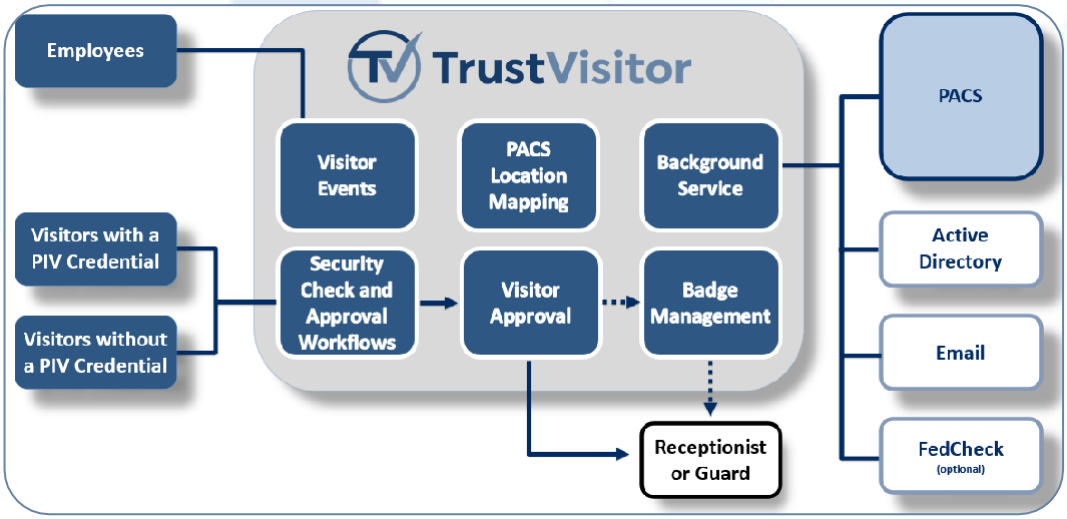
Customizable Visitor and Employee Pre-Screening

As facilities consider reopening their doors, employers need to decide whether, when, and *how* they will reopen while being mindful of their responsibility for the health and safety of their employees and visitors. Having the ability to ask customized wellness questions of individuals within hours of their arrival but before they enter a facility is highly desirable in the event that someone is unsuitable to be physically present in a location.

TrustVisitor enables clients to ascertain the wellness of employees and visitors through an extensive and highly configurable wellness screening feature. Facility operators may allow visitors to complete and submit online wellness questionnaires, or they can require that wellness screening be administered in person by a lobby guard who can record the results of any check and whether the results fall within allowable thresholds. This feature can be configured to prevent or suspend access for individuals who have not passed wellness screening.

Wellness screening is important for everyone entering facilities, whether they are employees or visitors. Using the same wellness suitability capability to screen all persons gives businesses and facility owners peace of mind and increases employees' confidence that their workplaces are safe as they return to on-site work.

Anatomy of a High-Assurance Visit



About CertiPath

CertiPath, Inc. is a Virginia registered small business founded in 2004 to solve one of the most difficult problems in online security: determining whether a digital identity validly represents a person or "thing" requesting access to a network. Trusted digital identities are critical to the security of networks, data, and facilities.

CertiPath is the federated trust authority for high-assurance identity and access control to sensitive assets in both physical and online environments. We have defined a common standardized set of policies and practices for establishing, managing, and securing Public Key Infrastructure (PKI)-based identity credentials that meet the most rigorous standards for identity, integrity, and trust.

CertiPath was the prime contractor holder for the GSA FICAM Program, which manages the GSA APL for PACS, and is the prime contractor holder for the USMS Physical Security and FICAM Program. CertiPath's high-assurance visitor management solution, TrustVisitor, is uniquely suited to help federal agencies achieve FICAM conformance and increase their cybersecurity posture.

At the heart of its success, CertiPath applies unparalleled experience to create a suite of innovative, scalable products and services that hold identities accessing an organization's network to the highest level of validation. Using these tools, we protect the investment our customers have made in implementing high-assurance credentials as a method of authentication to their critical assets. Our trusted line of products leverage the Trust Fabric, a secure interconnection of trusted participants CertiPath spent a decade helping to create, to ensure that only valid and vetted users can access our customers' assets.