White Paper

TrustVisitor by CertiPath:

Made to Meet Federal High Assurance Standards

Version 3.3.001

Public Key Infrastructure

Public Key Infrastructure's (PKI) use within the U.S. Government was anticipated, even in its early days, 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 been realized to a large extent.

Homeland Security Presidential Directive 12 (HSPD-12)[1], issued 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 utilized PKI; specifically, the PKI found on the 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, whether 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 their visitor control processes undermine the value and security of their new high assurance PACS, but lament the lack of an easy means to provision PIV credentials issued by other organizations into the local PACS or provide an interoperable PKI-based smartcard to visitors. This capability and security gap has been exacerbated further by the lack of federal guidance on managing visitors in a PIV-enabled PACS environment.

The release of NIST SP-800-116-1[4] provided much-needed guidance on visitor management; and **CertiPath's TrustVisitor** provides the means to close this security gap once and for all in a manner that meets the spirit and the letter of HSPD-12, SP 800-116-1, and most recently, M-19-17[5].

1 HSPD-12, *https://www.dhs.gov/homeland-security-presidential-directive-12*

2 FIPS 201, *https://csrc.nist.gov/publications/detail/fips/201/2/final*

3 M-11-11, *https://www.cac.mil/Portals/53/Documents/m-11-11.pdf*

4 NIST SP 800-116-1, *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-116r1.pdf*

5 M-19-17, *https://www.whitehouse.gov/wp-content/uploads/2019/05/M-19-17.pdf*

The Last Mile

A high assurance means of verifying the identity of visitors and the areas they subsequently access is a primary focus of HSPD-12. To accomplish this requires a PACS that has the capability to:

- understand if 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,
- provision the credential with the appropriate access level and for the duration of the visit and no longer.

Significant effort has been expended by the vendor community over the past ten 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[6] and its supporting Special Publications. A stated goal of HSPD-12, Memo 11-11, and Memo 19-17 is cross-organizational trust: the reliance on any one agency's PIV credential by any other agency's PACS. The industry delivered exactly what was asked of it, PACS that can accept credentials from multiple issuers across multiple agencies. However, little attention was given to the processes required for external credentials to become known/provisioned to the PACS. The entire subject area of visitor management was deprioritized 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 took notice of this technical gap. Just as OMB restated the intent of HSPD-12 in Memo 11-11, NIST has made clear the requirements and expectations for visitor management in SP 800-116-1, states the following in Section 6.7

"Temporary Badges – 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."

And goes further by providing 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."

The DoD came to this same realization in 2014. One of the 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.

6 FIPS 201-2, *http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf*

7 DTM 09-012, *https://www.hsdl.org/?abstract&did=800675*

Who and When

A visitor is person meeting someone or going somewhere at a location. The need for and scope of the visit is initiated by someone within the organization, an "event sponsor." This could be to attend a meeting or maintain some part of the facility. The event sponsor knows who 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. This is the starting point for any visitor workflow. The system needs to:

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

A visitor, in the context of HSPD-12, 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 where the access grant expires before the credential does

Wait … What?

The first of these two definitions is straightforward. The second one bears explanation. An HSPD-12 PACS understands a person by his credential number and the locations for which he has been granted access. The duration of the access grant begins with the day and minute the grant is established and expires contemporaneously with the person's credential. For routine access personnel this is appropriate. For visitors, even those who may be from the same organization but do not require routine access, this is likely not so. The date and time attributes of a visitor's access grant should reflect the duration of the approved stay. This is the primary distinction between routine access and visitor access.

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 becomes particularly useful when multiple facilities are correlated across a large geography.

If a visitor does not have a credential, gathering 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 a PIV or CAC 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 their 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 (i.e., the facility is 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 (i.e., CIV)
5. Locally issued non-personalized (i.e., Building Badge)

Where

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

Consider the following scenario: a sub agency 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 sub agency'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 sub agency, 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 question that must be answered. In fact, 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. This is 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, having a consistent and accurate source of information that explains why access was granted is not possible.

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 access points in between may very well be different again.

Putting it All Together With TrustVisitor

CertiPath's TrustVisitor is designed to permit security officers and PACS administrators to answer the 5Ws in a repeatable and automated fashion. With the TrustVisitor solution, all visitors interact with the same system; all visit requests are administered from the same interface.

Once the 5Ws are answered, TrustVisitor provides all the necessary provisioning information to the PACS (or to each of the PACS) associated with the visitor's approved access. No human interaction is required. For greatest control, approvers can be assigned at any level.

TrustVisitor is a point of aggregation for all the PACS across all the facilities in an enterprise. TrustVisitor 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 and more 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 ✓ sometimes supported ✓ fully supported

Supported Feature	Standard Visitor Management	Typical High Assurance Visitor Management	TrustVisitor
HSPD-12/FICAM compliant	X	✓	✓
Scheduled and unscheduled visitors	✓	✓	✓
Clientless email integration	X	X	✓
Background check integration	✓	✓	✓
Preregister an electronic credential remotely	X	X	✓
Visitor use of personal electronic credential	X	✓	✓
Assign a temporary electronic visitor credential	X	✓	✓
Provision tailored visitor access in facility access control system	X	✓	✓
Interoperable with multiple brands of PACS at one facility	X	X	✓
VIP visitors	✓	✓	✓
Touchless check-in via kiosk	✓	✓	✓
Employee and visitor wellness screening	✓	✓	✓
Assign a temporary credential for forgotten employee badges	X	X	✓

The TrustVisitor Experience

In a high assurance visitor management process, the event sponsor, visitor, approver, and lobby guard play the 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, email approvals, VIP processing, and kiosk self-check-in, TrustVisitor clients have found that over 95% of the people involved in their end-to-end visitor management process can complete their task 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.

Wellness

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 someone is already 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 an online wellness submission, or force wellness to be administered in person by a lobby guard who can record the results of any check and whether it was within allowable thresholds. This feature can be configured to prevent or suspend access to individuals who have not passed wellness screening.

Wellness screening is important for everyone entering facilities, whether employee or visitor. Having the same wellness suitability capability used to address all persons will create a reliable capability and increase confidence of employees returning to 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. The heart of CertiPath's success is our unparalleled experience with creating innovative, scalable products and services that ensure the highest levels of validation for digital identities that attempt to access customers' networks.

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

At the heart of our success, CertiPath applies our unparalleled experience to create a suite of innovative, scalable products and services that hold identities accessing your 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, the secure interconnection of trusted participants CertiPath spent a decade helping to create, ensuring your assets are being accessed by valid and vetted users.