Oct
2023

TrustVisitor®
Product Brochure

Version 4.1

Version 4.1.00

Background

The vendor community has expended significant effort over the past 15 years to bring robust, Personal Identity Verification (PIV)-enabled Physical Access Control Systems (PACS) to market to facilitate high-assurance physical access control for facilities that federal agencies use. A stated goal of Homeland Security Presidential Directive 12 (HSPD-12), Office of Management and Budget (OMB) Memorandum M-11-11, and OMB Memorandum M-19-17 is cross-organizational trust: the ability of an agency's PACS to rely on a PIV or Common Access Card (CAC) credential issued by another agency. Thanks to industry efforts, PIV-enabled PACS can accept credentials from multiple issuers across multiple agencies. However, little attention has been given to the subject of visitor management. Likewise, almost nothing has been done regarding high-assurance visitor management.

TrustVisitor is CertiPath's solution to federal high-assurance visitor management. The platform has been designed from the ground up for federal agencies to be compliant with HSPD-12, M-19-17, and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-116, Revision 1. TrustVisitor enables approved visitors who have been issued suitable credentials by either the same agency or another agency to be able to use those credentials to facilitate physical access to a facility for the duration of a visit. If approved visitors do not possess such credentials, they are issued temporary credentials that interoperate with the PACS in the same electronic fashion.

Automatic Provisioning for Limited Access

During the configuration process, TrustVisitor constructs a virtual map of available and approved facilities and locations. Working in conjunction with the PACS, the platform determines the correct path between a facility ingress point (e.g., the lobby) and the meeting/visit location. It uses this information to provision the visitor's credential for tailored access—only providing the access necessary to reach the target location and no other locations. This access is provisioned within the PACS just before the meeting start time (configurable; defaults to 15 minutes) and is deprovisioned just after the meeting end time (also configurable).

Supported Visitor and Employee Scenarios

- ✓ Scheduled visits, meetings, and conferences for visitors with and without PIV, CAC, or PIV-Interoperable (PIV-I) cards
  - If a visitor does not have a PIV, CAC, or PIV-I card, TrustVisitor collects sufficient information, via the visitor's government-issued photo ID, so that they can be identified and authorized to use the designated location upon arrival.
- ✓ VIP, Unscheduled, Unregistered, Employee visitors
- ✓ Fully customizable event and visitor workflows with user defined fields
- ✓ Issue Commercial Identity Verification (CIV) cards for employees that forget their PIVs or CACs

The TrustVisitor Process

The high-level, end-to-end TrustVisitor visitor management process follows these steps:

- Sponsors use their calendar tool to create high-assurance events and include TrustVisitor as an attendee.
- TrustVisitor uses the location and visitor info from the invite to automatically create the event and visit request.
- An automated email is sent to the visitors with a request to pre-register for the event via the TrustVisitor visit pre-registration portal.
- During pre-registration, the visitor's PIV, CAC, or PIV-I is read or their government-issued photo ID details are collected. The visitor also has an option to present their identification credential upon arrival for the event.
- Any necessary agreement documents are displayed to and accepted or rejected by the visitor during pre-registration.
- Visitor credentials are continuously validated from the time the visitor registers through the event date.
- Visitors can be required to submit wellness screening as part of the pre-registration process or during kiosk check in, or you may require visitors to submit to an in-person wellness screening.
- Prior to on-site arrival, approval(s) for each visitor are obtained via an email-based workflow. Alternatively, approvers can use TrustVisitor's Approver module to approve or reject visitors.
    - Custom approval workflows and user defined fields are set via admin workflow creation tool.
- Additional documents, including directions to the event location and a QR check-in code, or any customized notifications can be sent at any time in the process.
- Upon arrival, visitors can check in for their event on a kiosk in a touchless fashion by scanning a QR code or by presenting their PIV, CAC, or PIV-I.
- Visitors who do not possess high-assurance credentials are issued temporary credentials that are electronically interoperable with the PACS.
- Unregistered visitors can be registered as "Escort Required" in the lobby.
- Visitors designated as "VIP" may be granted temporary credentials.
- Unscheduled visitors may request a meeting at the Lobby Guard station or via kiosk.

User Access

TrustVisitor uses the approach described below to identify authorized users:

- TrustVisitor does not create its own user accounts or groups. Instead, it integrates directly with Active Directory and uses the existing accounts and groups within Active Directory.
- TrustVisitor provides for a role-based access model by allowing the System Administrator to map Active Directory groups to TrustVisitor roles.

Operating via the least-privilege model, once a user authenticates to TrustVisitor they are provided with a role-dependent view of system features and functions. Users only see functionality that they are given access to.

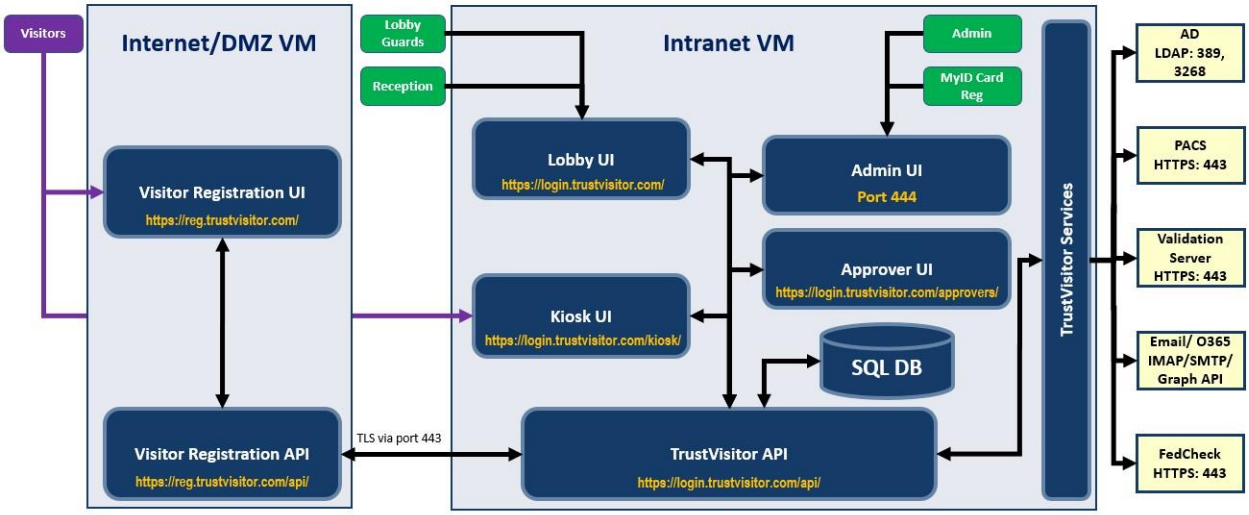
System Architecture

TrustVisitor is a secure web-based application that supports standard web browsers, eliminating the need to install any client software. Any user with a computer or device with network connectivity can connect to the system via a secure URL, authenticate via a credential, and be able to perform any of the system functions to which they have been granted role-based access.

The architecture is modular and scalable. Several components of the system can be moved to dedicated hosts or duplicated on multiple hosts to provide for scalability.

TrustVisitor is a modern 64-bit software solution that uses a microservice-based component model coupled with a SQL backend database and an efficient JavaScript framework-based user interface. The microservices are written in C# and rely on Microsoft's .NET framework. The services communicate via a REST API or a message queue, depending on the operation being performed.

TrustVisitor Conceptual Diagram – Production Deployment



All ports numbers shown are configurable

Integrations

- ✓ Microsoft Active Directory for Identity and Access Management (IAM)
- ✓ Microsoft Exchange for Calendaring and Scheduling (Both on premises and Exchange Online/O365)
- ✓ GSA Approved Products List (APL) PACS:
  - Tyco Security Products C●CURE 9000 v2.9 and v3.0
  - Lenel OnGuard v7.6 and v8.0
  - Gallagher PIV Command Centre version 8.50 and 8.60
  - Identiv Hirsch Velocity v3.7/SP2 and 3.8.2
- ✓ Ident Solutions FedCheck (optional background check service)
- ✓ GSA APL Validation Systems:
  - Innometriks 2.3.0.7 and 2.3.1.2 (Server) and 2.3.0.19 and 2.4.0.14 (HA Service)
  - HID® pivCLASS® 1.4.10 (multiPACS), 5.8.1 (pivCLASS client)

Compliant with the Following Specifications and Standards

- ✓ PIV, PIV-I, CAC, and CIV cards for visitors
- ✓ Supports HSPD-12, M-19-17, and NIST SP-800-116, Revision 1
- ✓ Fully supports the use of PIV authentication mechanisms with different location security levels

TrustVisitor Version 4.1 Highlights and Roadmap Features

Version 41.

- ✓ Enterprise multi-tenant support
- ✓ Set user access based on Scope

Future Roadmap

- Enhanced Admin UI
- Sponsor event management UI