TrustSuite™ Frequently Asked Questions

Identity Management System (IDMS)

What Identity Management Systems and other sources of identity information does TrustManager™ support?

TrustManager has been integrated using Lightweight Directory Access Protocol (LDAP), Microsoft Active Directory, Apache NiFi data stores, and the Intercede MyID® IDMS. Additional integrations are available upon request.

My organization has separate data stores for employees and contractors. Does my organization need a single system that manages both employees and contractors?

TrustManager supports multiple identity sources and relies on a single source of authority/source of truth *per identity*. The only requirement is for an identity to be provided by a single source. Separate sources can be used for employees, contractors, and other groups that may be defined by your organization's current business rules and policies.

TrustManager: Automated Identity and Credential Provisioning Within a Business Unit, Across Your Organization's Enterprise, or Across a Broader Community of Trust

Does TrustManager capture identity information to begin an identity record or add to an existing one?

TrustManager automates the facilitation of that process, based on your organization's existing identity management system or source of authority.

TrustManager assumes that a primitive identity record was established in the IDMS or other authoritative source as a starting point. This nascent record typically includes a minimal set of biographic data, such as Name, Role, or PersonType, and a unique identifier within the organization. TrustManager passes this partial identity record to a Credential Management System (CMS) such as Intercede MyID. A CMS improves the identity record by adding additional proofing, which provides corroboration of existing biographic data and captures additional biographic data, and by binding biometric image captures to the identity record. Lastly, one or more credentials are typically issued to the identity. TrustManager then manages the provisioning of the identity record and its associated credentials to supported access control systems.

What is identity proofing, vetting, and credentialing and where do these things occur in a FICAM or Zero Trust Architecture? How does TrustManager support all of this?

Organization credentialing typically begins with an "I-9" style process in which government-issued identity documents are reviewed as part of the onboarding process. Since many human resources departments are limited in their ability to detect fraudulent versions of the various forms of identity "breeder" documents, this document review is used only to start an identity record.

Many organizations require additional suitability checks before they offer an individual full-time employment or issue them a high-assurance credential. Although several variations of this process may be employed, TrustManager hands off the initial identity record to a CMS as described previously. The CMS supports robust identity proofing that typically involves the presentation of breeder documents and a higher level of inspection to discern counterfeit documents. This process may include verification by the document's issuer.

The CMS populates the record with additional biographic elements and uses automated and secure collection to capture and store biometric images. These additional attributes typically include facial images and fingerprints but may optionally include iris images. (Note: Additional biometric captures are possible if required by your organization, but they would be CMS vendor-specific and unlikely to interoperate within a trust community.)

The CMS processes the biographic and biometric identifiers as captured and passes them to background service providers (often called ISPs) in a personnel security process that is referred to as identity vetting or suitability checking. "Suitability" can be used to describe more than a person's past behavior as a predictor of future performance; hence "vetting" is a more specific term to describe a background check.

All of these actions take place within your organization's CMS. When proofing and vetting requirements have been successfully met, one or more user credentials are issued. TrustManager then picks up the improved identity record and associated credential records and securely provisions them to configured access control systems according to your organization's defined business rules.

Can I use TrustManager to provision access across multiple facilities?

Yes. TrustManager can provision to multiple access control systems at multiple sites and facilities. TrustManager supports both enterprise and standalone Physical Access Control System (PACS) architectures.

Can I use TrustManager to provision credentials to a partner organization's PACS as part of my Community of Trust? Can I receive automated provisioning of identities and credentials from a trusted community?

Yes. This "FICAM v2" advanced use case for Communities of Trust is supported. TrustManager leverages a publication-subscription model and, when used in conjunction with CertiPath's TrustMonitor™ and the Intercede MyID CMS, will equally support automatic PACS provisioning of identity credentials from your own organization and those issued by any other trusted community member.

Intercede MyID: The Most Versatile and Secure Credential Management System

Does MyID as a CMS directly issue and manage user credentials?

Yes. The MyID CMS software solution issues and manages user credentials, with support for a broad range of enrollment workstation, biometric scanner, and document scanner hardware.

Is there a vetting-process workflow that occurs before a credential is issued?

Yes. The MyID CMS is most often responsible for the employee vetting process. Visitors to your organization may be vetted via the CertiPath TrustVisitor™ application.

For employees, we leverage the biometric adjudication module within MyID. This MyID module workflow takes fingerprints in EBTS formats (rolls and prints are both supported) and submits them to various biometric ISPs. Biographic ISPs can be supported as well for things like Criminal History Record Check (CHRC). When the vetting workflow is deployed, MyID waits for a positive adjudication response before continuing with the issuance workflow.

For visitors, TrustVisitor serves as the IDMS, CMS, and TrustManager for individuals who are not in the enterprise IDMS. TrustVisitor supports biographic ISPs (non-biometric) for things like CHRC. When a facility employs vetting for visitors (or just certain types of visitors), TrustVisitor will prevent a visitor from receiving a credential or access until it receives a positive adjudication response.

For high-assurance smart card issuance, is there a recommended Certificate Authority (CA), or are there requirements for the CA itself?

TrustSuite supports most commercially available Public Key Infrastructure (PKI) CAs. However, if your organization intends to participate in a formal Community of Trust, it is important to select a CA technology that is capable of cross-certification (e.g., EJBCA, Entrust, RedHat).

Does the CA or CMS utilize a Hardware Security Module (HSM)?

Yes. Both the CA and the CMS require secure key generation and management as part of high-assurance credential issuance (not just the smart card-based keys within a person's credential). These are best protected by an HSM. Please keep in mind for interoperability that each Community of Trust establishes requirements for HSM certification–frequently FIPS 140-2/3 Level 3 for CAs.

MyID feeds credential data back to TrustManager. Is TrustManager the customer interface for adding, revoking, and replacing credentials?

MyID notifies TrustManager that a change has occurred, and TrustManager processes each change via a publisher-subscriber model. However, all credential management is conducted within the MyID application.

TrustZero™: Credential Validation Reengineered

What access control systems does TrustZero work with?

TrustZero has been integrated with the following:

- LenelS2's OnGuard®. Specifically, there is a variant of Lenel/Mercury's x4420 panel with TrustZero firmware.
- Software House's C•Cure™. The iSTAR Ultra panels are supported.
- For organizations with existing deployments of HID pivCLASS®, some of the TrustZero capabilities can be achieved with other TrustSuite components. TrustManager supports provisioning to pivCLASS, and, when combined with TrustMonitor, will achieve real-time validation with no other changes to the current PACS deployment. Other FICAM v2 features would require switching the validation component to TrustZero.

Is TrustZero a server application?

Yes. TrustZero will most often run on the same server as the PACS head end, but it can be deployed onto a separate physical or virtual machine (VM) on the same network segment as the head end. TrustZero manages its own database of credentials bound to identities, which will consume some system resources.

Is TrustZero also firmware that resides on the panel?

No. TrustZero must either talk directly to panel firmware or do so through a PACS head end service. These approaches are the basis of integration between a validation system and a PACS. In the case of Mercury controllers, HID Global has developed specific TrustZero firmware. Software House employs a panel service that abstracts the panel firmware for any validation system interoperating with it, resulting in TrustZero supporting the standard iSTAR Ultra hardware.

Does TrustZero communicate with TrustMonitor to get updates and validations for credentials that were issued by another facility?

Yes. TrustZero communicates with a TrustMonitor instance using mutually-authenticated Transport Layer Security (TLS) via Internet-standard ports and protocols.

TrustVisitor: FICAM-Compliant High-Assurance Visitor Management

Does TrustVisitor reside on top of or beside this configuration for visitor management?

TrustVisitor runs in parallel and separately from the other TrustSuite components. As described previously, TrustVisitor fulfills the role of IDMS, CMS, and TrustManager for your organization's visitor identities. TrustVisitor leverages whatever validation system is tied to the specific PACS it is serving; it does not use its own validation system.

Does TrustVisitor have an event management capability?

TrustVisitor currently does not include a formal event management function. This has been a conscious choice. Each time we have examined how event management is conducted at otherwise high-security facilities, we have found that it largely has been implemented as a means to circumvent the visitor security policy to handle large numbers of event visitors. We continue to evolve our approach to events.

The current version of TrustVisitor serves a large event in the following way:

1. A sponsor (or sponsors) creates the meeting/event.
2. This meeting/event record can invite hundreds or thousands of people via email.
3. A portion of those people use the visitor registration link they receive.
4. The portion who do not pre-register for the event must register onsite with the lobby guards or at a TrustVisitor kiosk.
5. Some would-be attendees show up who were not part of the original invite list. Those people need to interact with the lobby guards to determine if they should be admitted to the event. TrustVisitor supports escorts for uninvited but now-registered people if the facility enables this option.

In a release scheduled for 2024, a sponsor interface will enable the creation of meetings and events outside of Outlook. This is expected to further improve the invitation process for events as part of the TrustVisitor product roadmap.

Cards and Printers

Is there a published list of ”Approved” cards and card printers?

Yes.

TrustSuite with MyID is compatible with all FIPS 201 approved smart cards. TrustSuite with MyID also supports Corporate 1000 proximity credentials, both as standalone proximity tokens and as proximity inlays within the card body of a smart card.

Please refer to the current Intercede MyID printer compatibility matrix for a full set of approved card printers. MyID generally supports Entrust Datacard and HID Fargo and has newly added support for IDP printers. We recommend using a printer that has a USB interface and an embedded smart card encoder. Laminators also significantly prolong the printing on a smart card if surface printing is desired.