



**Identity
Management
for
Critical
Infrastructure**

TrustSuite

CertiPath

- **Federated trust authority** for High Assurance identity and access control to sensitive assets
 - Defined a standardized set of policies and practices for establishing, managing, and securing **Public Key Infrastructure (PKI)**-based identity credentials
 - Prime contractor holder for the **GSA FICAM Program** which runs the GSA APL for PACS and for the **USMS Physical Security and FICAM Program**
- **TrustSuite** is uniquely developed to enable **Energy sector** clients seeking to achieve conformance and increase their cybersecurity posture

**Are your credentials
SECURE?**

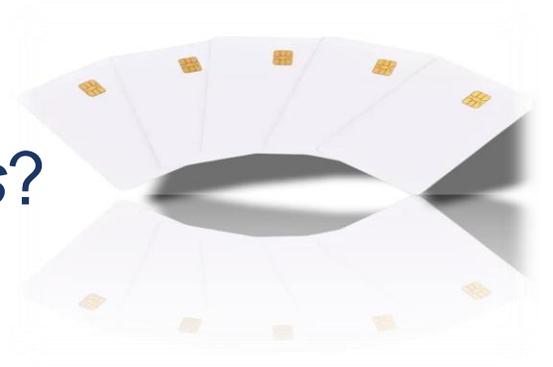


**Are your ID processes
a MANUAL BURDEN?**



You trust your strong **locks**...

Do you trust everyone's **keys**?



If a KEY is not SECURE, you need to know immediately!

TrustSuite's industry-leading feature set delivers HIGH ASSURANCE and AUTOMATES your entire identity management process.



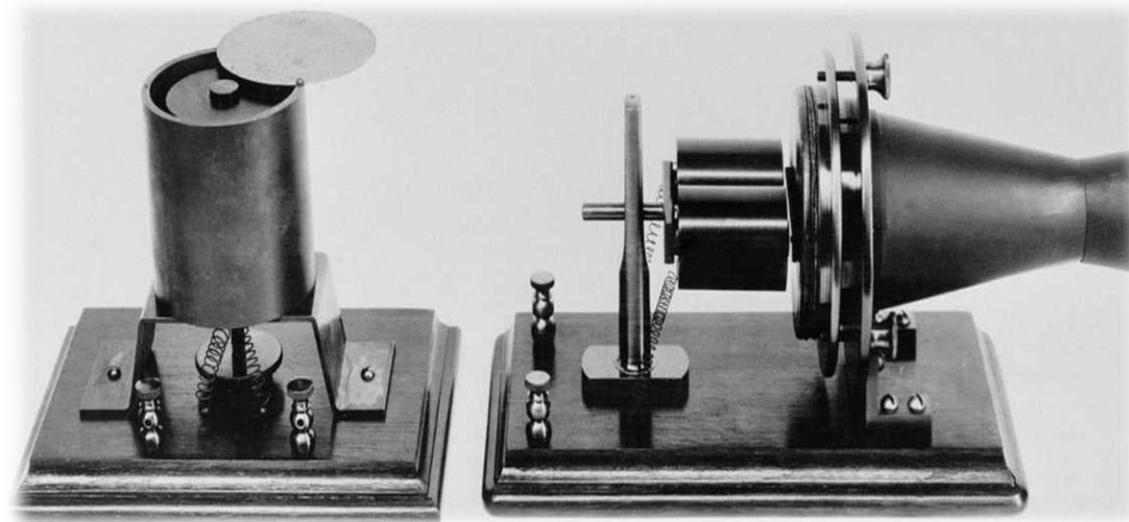
Your fortified premises must not become a house of (prox) cards

The “Good” News

The **technology** to apply High Assurance PKI identity management **policy** has been available for *decades*

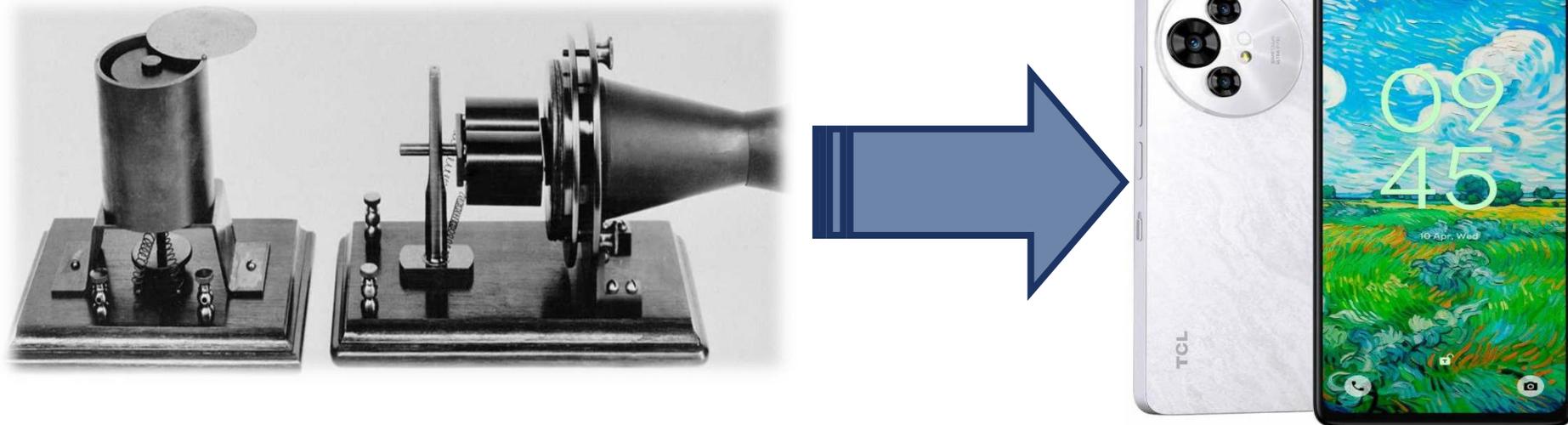
The Bad News

The **process** has always placed excessive **burden** on the people who support, operate, and implement it



CertiPath Has GREAT News!

Our singular focus is to make
High Assurance identity management
enterprise class for critical infrastructure clients,
with **automation** for common tasks to make
policy effortless to live with day to day

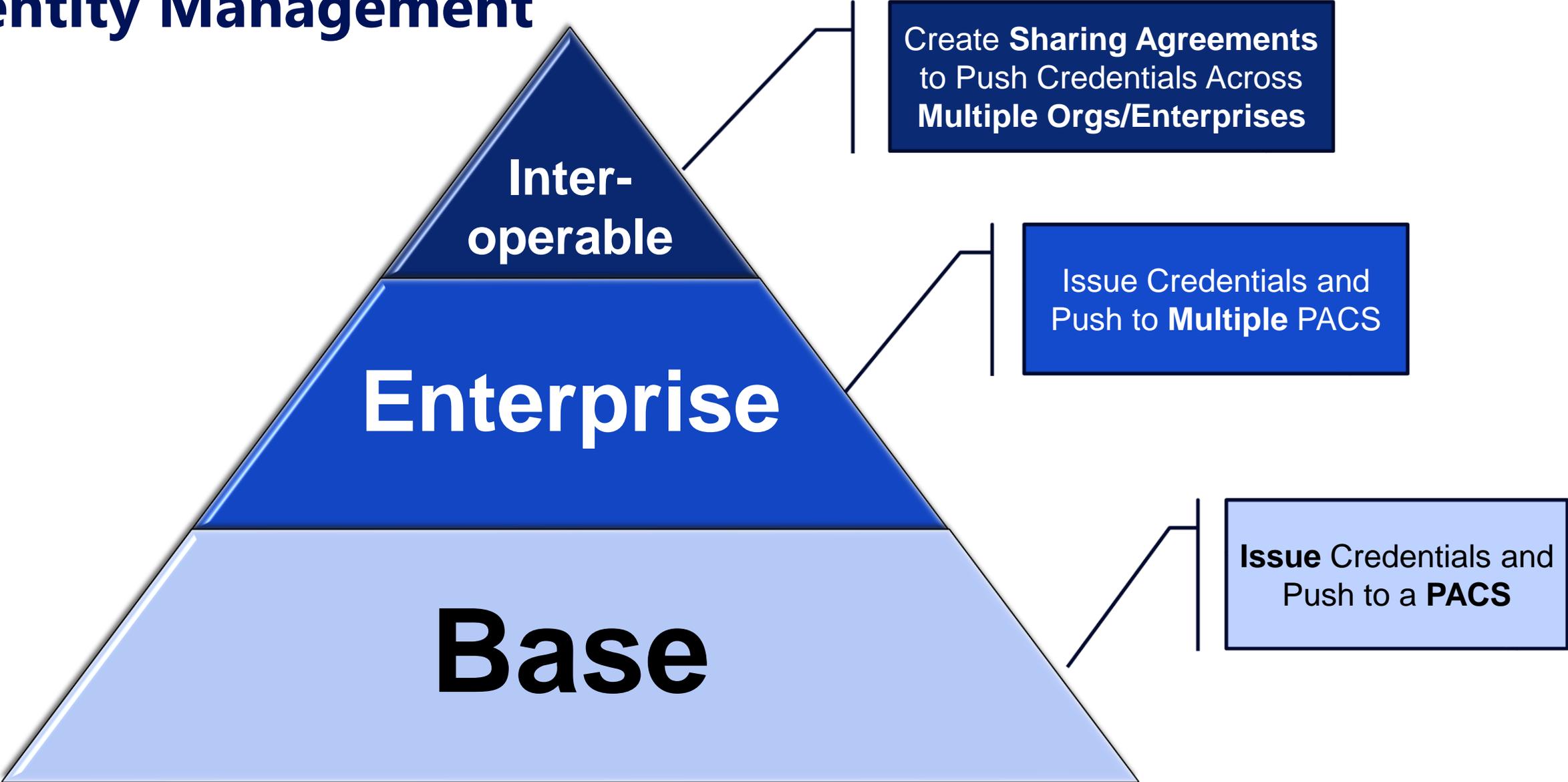


CertiPath Has GREAT News!

Our **services** team builds compliance across isolated departments inside your org to make it **easy** to go from low assurance prox cards to utilizing **High Assurance** credentials



Evolution of Energy Identity Management



Key Features

TrustManager

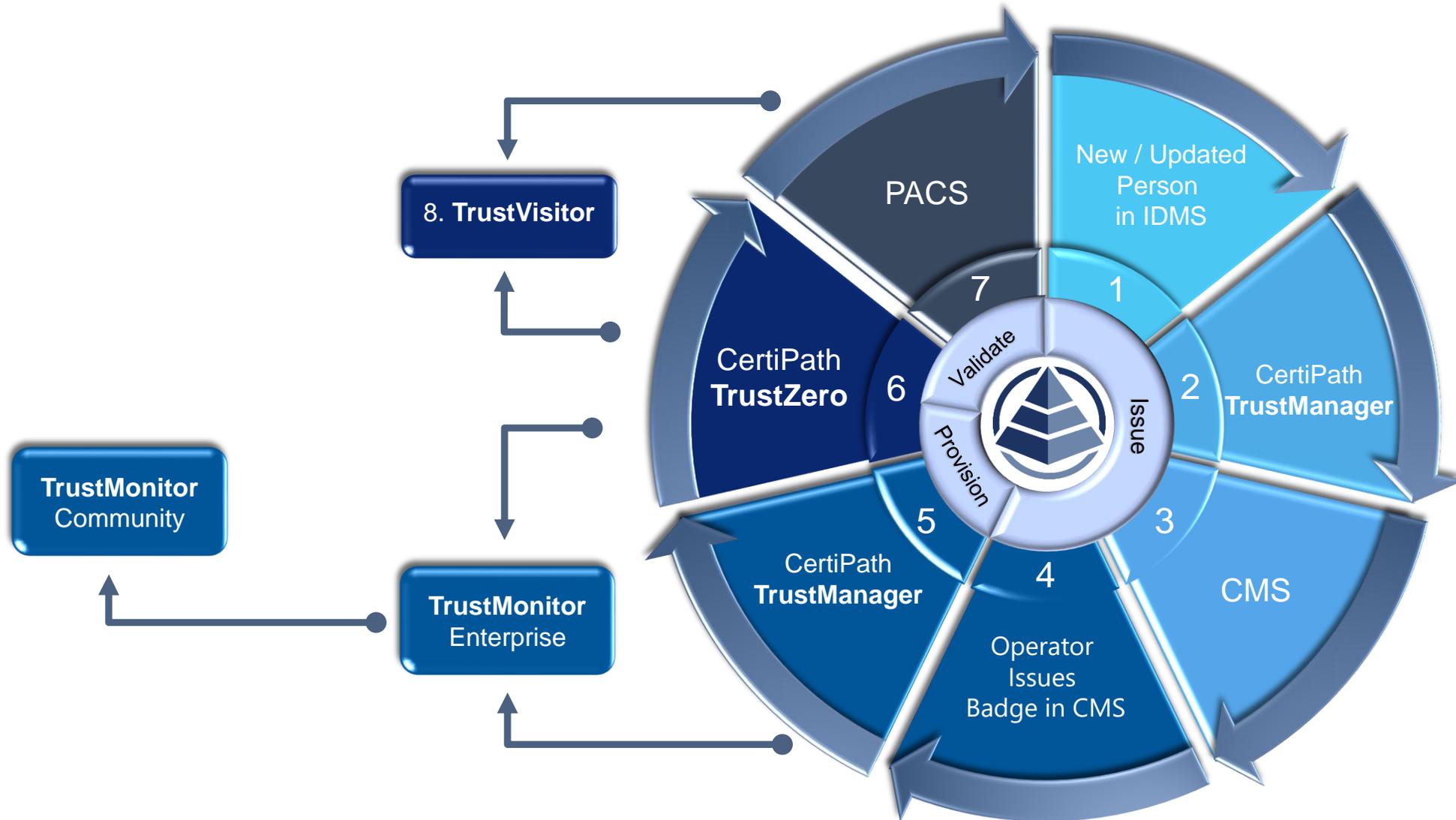
TrustMonitor

TrustZero



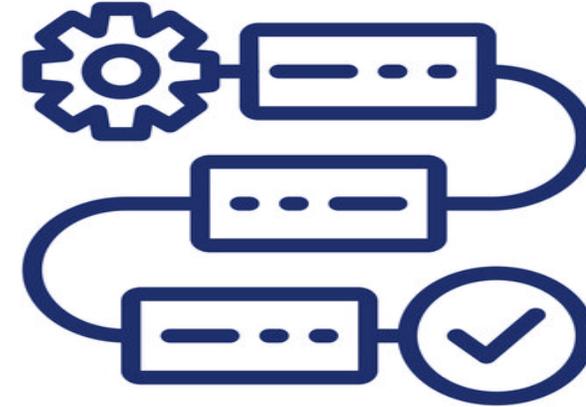
TrustSuite
CertiPath

TrustSuite Issuing, Provisioning, and Validation Activities



TrustManager Overview

TrustManager is CertiPath's integration solution for provisioning of **Energy sector identity records and credentials** across PACS. TrustManager's custom **workflow** tool connects all phases of the **identity lifecycle** in one centralized application.



TrustManager, when paired with TrustMonitor, delivers **intercommunity provisioning** to support several disparate organizations **across the Energy vertical** that share a trust relationship to form a community.

Our solution provides **automated**:

- Physical access rights to each community member's employees
- Updates or removal of access when appropriate

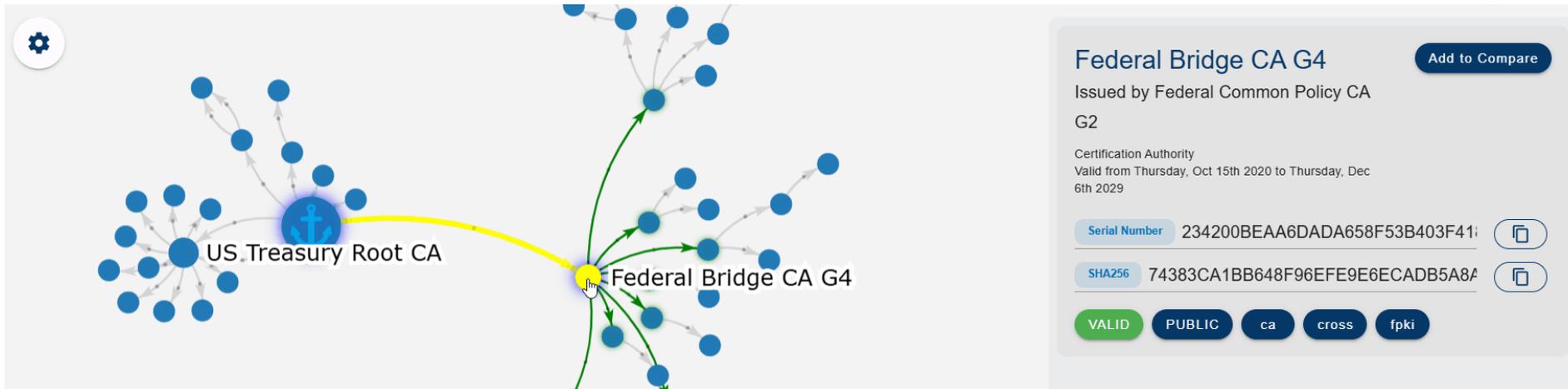


TrustManager Feature Summary

- ✓ **FICAM v2** physical identity access manager
- ✓ **Automatically** provision/update/deprovision identity and credential records to any PACS
- ✓ Compatible with all **PIV** applet-based, **proximity-based**, and **dual-hybrid** credentials
- ✓ **Workflow** tool to customize connections to multiple APIs:
 - Pull credential information from CMS or legacy systems
 - Transform data to send to other operational systems
 - Automate intercommunity federal provisioning
 - Receive and send secure system transactions (SFTP)
 - Configure pre/post processing rules
 - Troubleshoot workflows: maintenance mode, exception handling/retries
 - Compare/reconcile/remediate data sets across multiple systems

TrustMonitor Overview

- Public, community, and enterprise-specific settings
- Near-real time validation of credentials
- Focuses on PKI credentials and issuers
- Private instances for any roots of trust an enterprise/community may also wish to monitor



The image displays the TrustMonitor interface. On the left, a trust path diagram shows a central node labeled "US Treasury Root CA" with an anchor icon, connected by a yellow line to another central node labeled "Federal Bridge CA G4". Both nodes have multiple smaller nodes branching out from them, representing a hierarchy of certificates. On the right, a detailed view of the "Federal Bridge CA G4" certificate is shown. It includes the text "Issued by Federal Common Policy CA G2" and "Certification Authority Valid from Thursday, Oct 15th 2020 to Thursday, Dec 6th 2029". Below this, the "Serial Number" is 234200BEAA6DADA658F53B403F41 and the "SHA256" hash is 74383CA1BB648F96EFE9E6ECADB5A8A. At the bottom of the panel, there are several status tags: "VALID" (green), "PUBLIC", "ca", "cross", and "fpki". An "Add to Compare" button is located in the top right corner of the certificate details panel.

- Proactively tracks and “pushes” updated credential information to achieve quicker propagation and synchronization of credential status changes
- Streamlines the configuration of the trust path, ensuring accurate status
- Enables configurable constraints at a global and local level when using TrustZero

TrustZero Overview

TrustZero is CertiPath's **high-assurance** credential **validation** solution that provides robust **business logic** and **configurability** for a PACS' response to a range of validation conditions

The Problem: Dangerous Validation Time Lag

Current validation systems suffer from “**revocation blindness**,” a credential revocation typically takes **36 hours** to impact what happens at a door.

The Solution: TrustZero & TrustMonitor

Achieve near real-time knowledge of credentials via a sophisticated layer of status-checking techniques, which reduces this operational blind spot to **2 minutes**.



Would you hire blind Security Officers?



Would you give Lobby Guards 36-hour breaks?

TrustZero and TrustMonitor Feature Summary

- ✓ Enterprise-level **continuous validation**
- ✓ **Near-Real-Time revocation**
- ✓ **VIP** privileged credentials
- ✓ Configurable **extended validity period / degraded mode** settings
- ✓ Validation **enforcement** options
- ✓ **Single network** location for all validation queries
- ✓ Validate all credentials within complex **trust communities**
- ✓ **Realtime automated trust list pruning** with no manual checks

TrustManager and TrustZero PACS Integrations

TrustManager



TrustZero



Key Features



TrustVisitor[®] Overview



TrustVisitor is CertiPath's solution for **high-assurance visitor management** for **critical infrastructure** facilities. TrustVisitor determines who a visitor is and then evaluates what **credential** they possess and if it will interoperate with all **PACS access points** the visitor will traverse.

The platform has been designed from the ground up with a specific view toward **high assurance** compliance. TrustVisitor helps organizations achieve **compliance** with HSPD-12, M-19-17, and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-116-1.

TrustVisitor Workflows: Power + Flexibility

■ Visitor Information

- Customize visitor registration by location

■ Workflow Evaluators

- Register with a Smart Card?
- New or Returning Visitor?
- Accept Agreement?
- Response to any User Defined Field

■ Actions

- Require Custom Approval Step(s)
- Require Background Check
- Auto Approve
- Auto Reject
- Customize an Existing Notification
- Create a New Notification
- Require Event Preauthorization

■ User Defined Fields (“UDFs”)

- Set as Mandatory/Optional
- Set visibility to Lobby Guard and/or Approver
- Tooltip/Help Text
- Interactive preview window
- Customize display order
- Library for common values (states, countries)

■ Supported User Defined Field Types:

- Date
- Display Text
- Display URL
- Drop Down Select
- File Upload
- Switch/Check Box
- Free Text
- Radio Button

TrustVisitor Feature Summary

- ✓ Orchestrate and automate disparate visitor management processes with **workflow customization**
- ✓ Tailor data collected during visitor registration, by location, via **user defined fields**
- ✓ Automatically create high-assurance events through a **calendar tool**
- ✓ Accept and **validate** visitors' electronic credentials from pre-registration *through* the event start time
- ✓ Approve/Reject visitors via **email** or through an **Approvers module**
- ✓ Integrate with any **background check** service, with option to **re-run** background check on demand
- ✓ Automatically provision approved visitors into the PACS for the **duration of their event**
- ✓ Provision **temporary credentials** to non-smart card visitors or to employees who forgot their badges
- ✓ Provide access quickly and easily to **VIPs** and to **Unregistered** and **Unscheduled visitors**
- ✓ Enable visitors to check in for events via a touchless **kiosk**
- ✓ Print **paper** visitor badges
- ✓ View badge status and visitor history **reports**
- ✓ Bind a **scanned ID** to a visitor record or create a **new visitor record** from an ID scan

TrustVisitor Integrations

PACS



Validation Systems





TrustSuite

Feature Summary

CertiPath

➤ Your “**keys**” integrator

✓ **Trust** your locks and keys

➤ Simplifies **High Assurance** credentials

✓ **Remove** dependency on **prox** credentials

➤ **Automates** the full credential enablement process

✓ **Eliminate** manual **PACS/Badging enrollment** stations

➤ Accommodates **High Assurance credentials** and **PACS** for all types of **employees** and **visitors**

✓ Secure **employee** badges on **day 1**, ensure **visitor** badges have **tailored provisioning** for visit

➤ Supports **full High Assurance** credentials and PACS, and those that have **yet to fully migrate** to High Assurance

✓ Transition to **high assurance compliance** at your pace based on your organization’s unique **risk tolerance** and **readiness**

TrustSuite

TrustManager/Zero/Monitor Differentiators

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

| Feature | Typical Identity/ Access Management | TrustManager | TrustManager with TrustZero/TrustMonitor |
|---|--|--------------|---|
| Manage identity and access across diverse PACS infrastructure, including intercommunity federal provisioning, for e2e identity lifecycle management | X | ✓ | ✓ |
| Leverage data from smart cards to establish a common identity across government agencies | ✓ | ✓ | ✓ |
| Interoperable with multiple IDMS, CMS, and PACS | ✓ | ✓ | ✓ |
| Automate policy across enterprise to eliminate multi-organization or community policies | ✓ | ✓ | ✓ |
| Workflow tool for custom API connections | X | ✓ | ✓ |
| Continuous, near real-time validation of credentials and disables revoked credentials in PACS in near real-time | X | ✓ | ✓ |
| Smart card login authentication | X | ✓ | ✓ |
| Full support of standalone proximity-based credentials and dual-hybrid smart card/prox tokens | X | ✓ | ✓ |
| FICAM compliant | X | ✓ | ✓ |
| Supports Zero-Trust security model | X | ✓ | ✓ |
| Single application /lower total cost of ownership | X | ✓ | ✓ |
| Robust business logic tools to automatically enforce access management policies | X | ✓ | ✓ |

TrustVisitor Differentiators

Key:  NERC Requirement **X** not supported  partially supported  **FULLY SUPPORTED**

| Feature | Commercial Visitor Management | Typical High Assurance Visitor Management |  TrustVisitor |
|--|---|---|--|
| Require an electronic credential (card key) for access | X |  |  |
| Ability for visitors to register a personal credential or have a temporary visitor credential assigned | X |  |  |
| Provision tailored visitor access in facility access control system with continuous validation | X | X |  |
| Interoperable with multiple PACS at one facility | X | X |  |
| Intuitive UI for security personnel |  |  |  |
| Secure visitor activity logs , with reports detailing date and time of interaction with access points | X |  |  |
| Point of contact for escorted and unescorted visitors | X |  |  |
| Fully HSPD-12/FICAM compliant | X | X |  |
| Scheduled, unscheduled, unregistered, VIP visitors |  |  |  |
| Clientless email and calendar integration | X | X |  |
| Background check integration | X |  |  |
| Fully customizable event and visitor workflows , driven by user defined fields | X |  |  |
| Touchless kiosk check-in |  |  |  |
| Assign a temporary credential for a forgotten employee badge | X | X |  |

CertiPath

For additional info,

[click here](#)

to visit our TrustSuite Info Portal

IDENTITY



WITHOUT
COMPROMISE

