TrustMonitor®: The Value Proposition for Continuous Monitoring of PKI Services

Overview

Public Key Infrastructure (PKI) solutions are ubiquitous in the online environment. As a technology solution, nothing surpasses PKI for its ability to provide authentication, data integrity, technical non-repudiation, and confidentiality for electronic transactions across organizational boundaries in a federated community of trust. Increasingly, organizations are relying on high assurance PKI to log into workstations, digitally sign communications, and protect sensitive information.

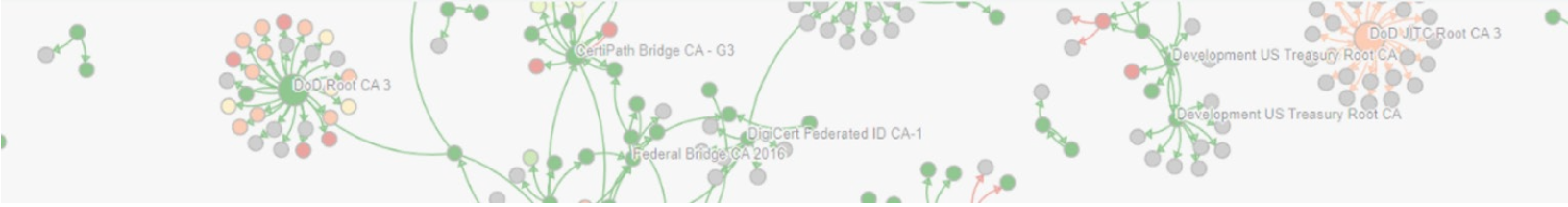
Unfortunately, the increased reliance on PKI makes it a tempting new target for identity fraud, denial of service attacks, and other cybercriminal activities. This is further complicated by the fact that, unlike the traditional network infrastructure, federated PKI is not fully contained in-house; by its very definition, the federated PKI trust community is a cooperative venture between multiple independent PKI domains. In other words, federated PKI represents a secondary network, largely existing outside the control of local system administrators, for whom the ability to predict failure and determine root cause are largely nonexistent.

> CDM capabilities are tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first.

Traditional network and system monitoring tools do not take into account those portions of the federated PKI trust community that are outside an organization's direct control. However, to ensure the continued integrity of daily business workflow, the organization must have the ability to implement Continuous Diagnostics and Mitigation (CDM) across this PKI trust fabric, which in turn will build confidence in the health of the PKI systems and processes on which the organization bases its trust.

CertiPath's TrustMonitor is the only product available today that is specifically designed to provide CDM for the PKI trust fabric. TrustMonitor tracks activity across the federated PKI trust community to verify that business-critical components are authentic, reliable, and available whether they are hosted internally or belong to an external member of the trust community.

TrustMonitor provides the organization with access to both real-time and historic trend information relating to specific incidents and overall PKI health through monitoring and analysis of the federated PKI trust community. TrustMonitor's reporting and alert features assist with incident response handling, threat mitigation, and planning/support activities. These capabilities ensure that productivity and security are not compromised by system anomalies or deliberate attacks on internal, external, or perimeter PKIs. The organization can use the unprecedented level of awareness into PKI-related dependencies and risks that TrustMonitor provides as a key resource in administering its mission-critical network infrastructure while gaining invaluable insight into the federated trust community.



TrustMonitor Use Cases

There are four core groups involved in the administration of the federated PKI trust community, each with system/network monitoring responsibilities:

1. Issuers of PKI credentials
2. Relying parties
3. Bridge certification authority administrators
4. Independent auditors

The following content discusses the use case for TrustMonitor as it applies to each of these groups.

Issuers

Issuers care about their part of the federated trust community, the certification authorities (CA) that they are responsible for, the certificates they issue, and little else. Although their scope of interest in the trust community is relatively small, the period over which they must maintain the integrity of the PKI is very long – generally in excess of 20 years.

Issuers convey individual credential trust via public directories containing information about credentials that have been terminated before their expiration dates. These certificate revocation lists (CRL) are the issuer's authoritative record of individual certificate validity. If a specific certificate has *not* expired and is *not* listed on the CRL, it is valid.

To be effective, CRLs must be short lived and new CRLs must be published before the expiration of the one preceding. A CRL's lifetime may be measured in hours as opposed to the months and years associated with a certificate's lifetime. If a CRL is allowed to expire without publication of a valid replacement, certificates associated with the CRL's issuer will be rejected by relying party applications, resulting in a denial of service for the certificate holders.

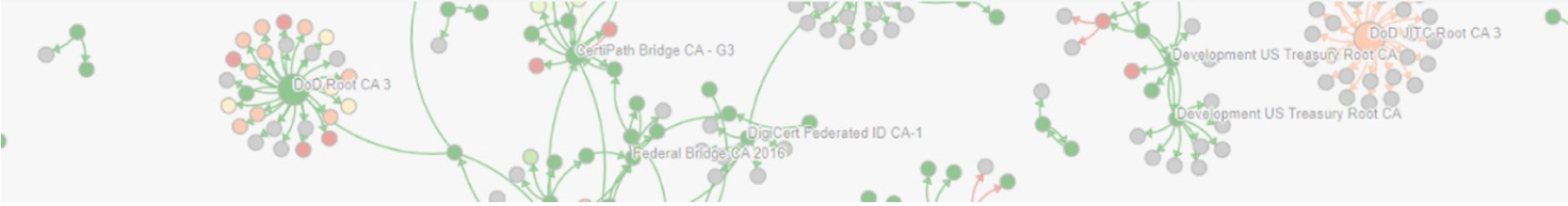
Therefore, issuers must continually monitor posted directory information for:

- **Timeliness:** Specific focus on the timeliness of revocation information is available via CRLs and their Online Certificate Status Protocol (OCSP) responders
- **Accuracy:** Posted information is accurate and unexpired
- **Integrity:** Directories have not been tampered with
- **Availability:** Revocation and directory information is accessible at all times

TrustMonitor is the *only* tool that provides in-depth continuous monitoring services that can be leveraged by PKI issuers, including evidentiary reports against timeliness, accuracy, integrity, and availability of directories. In addition, TrustMonitor provides active alerts whenever an anomaly related to a designated CA is detected (for example, when a CRL is about to expire and a new CRL has not been posted).

Relying Parties

Relying parties' acceptance of PKI credentials depends on trust. This trust often is given blindly, sometimes due to reliance on another entity such as the browser Trust Store. At other times, this trust is based on a relying party's extensive review and testing of an external PKI. However, regardless of what means was used to establish trust initially, generally nothing is being done to ensure that trust is still warranted; in other words, there is no CDM for trust. TrustMonitor is the *only* tool that provides this up-to-the-moment monitoring capability.



TrustMonitor gives relying parties a significant level of insight into the current status of the federated PKI trust community and provides early warning of failures that may impact PKI-credential–enabled access to a network, system, facility, or building. TrustMonitor provides early warning of trouble before it results in an unintended denial of service. At the same time, TrustMonitor keeps relying parties apprised of the overall health of the federated PKI trust community.

For relying parties, a failure in the federated PKI trust community that denies a user access usually results in a call to the Help Desk. Anything that reduces the Help Desk load can result in significant cost savings. Relying party monitoring of the federated trust community using TrustMonitor provides a substantial, measurable return on investment by heading off potential problems before they result in a Help Desk call and providing quick assurance to Help Desk personnel that the problem lies elsewhere.

Bridge Certification Authorities

Bridge certification authorities (bridge CAs) are an integral part of the federated PKI trust community. They function as Trust Framework Providers and are the cornerstone of the federated trust community. The benefits of a bridge are obvious. Without a bridge model, four CAs that want to inter-operate would each have to negotiate interoperability with each other, resulting in six sets of cross certificates paths; six CAs would have to create fourteen separate cross-certificate paths, etcetera. Replacing this direct-trust model with a bridge means that each CA requires only one interoperability relationship – between itself and the bridge.

A bridge issues cross certificates to independent PKI domains and receives cross certificates in return from each of the PKI domains. The bridge's primary focus is to facilitate cross organizational trust by creating a 'bridge' between the independent PKI domains and establishing a trust path between them. To be effective, bridge directory services must be available at all times. Therefore, bridge CAs monitor their directory services and ensure that they are online 24 hours a day, 7 days a week, every day of the year.

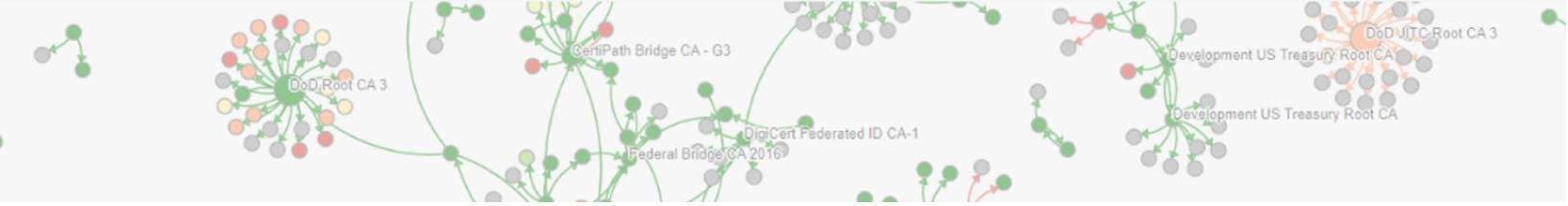
Issuers and relying parties must have timeliness, accuracy, integrity, and availability of bridge directory and revocation information in order to successfully discover and validate trust paths. This provides a further incentive for the bridge CA to understand the state of each of its member PKI domains and head off any potential situation that can upset the discovery and validation of trust paths.

TrustMonitor is the *only* tool that provides evidentiary reports against timeliness, accuracy, integrity, and availability of directories that can be leveraged by bridges. TrustMonitor puts a bridge in the unique position of being able to see broadly into the federated trust community and work with its members to mitigate risks before they impact other issuers and relying parties. TrustMonitor provides early warning of potential failures within the trust community connected to the bridge. TrustMonitor extends visibility of the bridge to all of its directly and indirectly connected community members to avoid these failures entirely or remediate them before they can develop into substantial interoperability failures in the trust fabric.

Independent Third Party Auditors

Independent third party auditors provide an important service to the federated trust community. Federated trust is based on the comparability of policy declarations concerning the operational environment. Independent third party auditors attest to the accuracy of these declarations as they pertain to a PKI issuer's operations.

A policy compliance audit tool must have reporting and summation over a number of controls based on the operations of the PKI, including CRLs and OCSP responses. Given that an audit typically covers a



1-year period, the auditor must rely on audit logs and other artifacts provided by the PKI issuer to determine whether the issuer has met its compliance objectives. This is an important component of a successful audit.

TrustMonitor is the *only* tool that provides evidentiary reports against timeliness, accuracy, integrity and availability of directories for the entire period of an audit. Its historical data allows an auditor to view the state of the PKI and the contents of its CRL at any point in the audit period.

Summary

Public Key technology is a powerful tool that enables our cybersecurity defenses. PKI issuers that participate in the federated community become part of a larger fabric of trust, a web of interconnected bridges, responders, and directories that are interoperable with each other. Relying parties decide to accept PKI-based assertions based on their trust of the federated community, bridge CAs provide the infrastructure that enables the federated community, and independent third party auditors provide an annual attestation that builds and maintains trust in the federated community.

However, as the federated trust community gains traction as a trust mechanism for online business transactions, it also becomes a target for cybercriminal activities. It is no longer sufficient to establish the trust relationships once and rely on an annual spot-check for continued integrity. It is time to take to take trust to the next level. It is time to employ CDM in the PKI federated trust community. CertiPath TrustMonitor does exactly that. For the first time, the trust fabric can be visualized in real-time and the federated trust community can be monitored for events that are occurring or are about to occur.

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.

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.