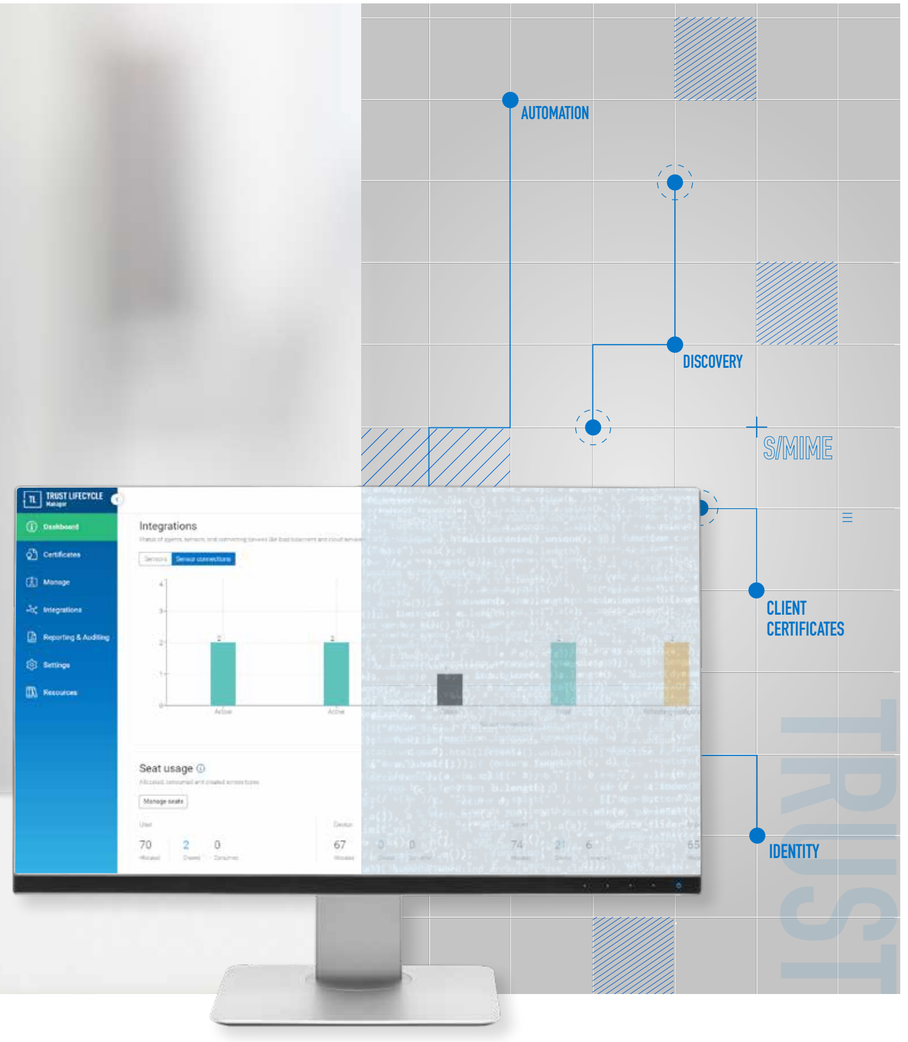
TRUST LIFECYCLE MANAGEMENT

HOW DIGICERT® TRUST LIFECYCLE MANAGER IS TRANSFORMING WHAT CUSTOMERS CAN EXPECT FROM CERTIFICATE LIFECYCLE MANAGEMENT



digicert®

01

TRUST LIFECYCLE MANAGEMENT

Author
Diana Jovin and Sean Crouch

Date
03-02-2023

Reviews
★★★★★ 124

02

TABLE OF CONTENTS

THE CONFLUENCE OF MARKET TRENDS IS DRIVING INCREASED INTEREST IN DIGITAL TRUST AS A STRATEGIC INVESTMENT RATHER THAN A UTILITARIAN BACKROOM FUNCTION.

RELATED RESOURCE

REDUCE THE RISK OF BUSINESS DISRUPTION

INTRODUCTION

THE PROBLEM: INCREASING COMPLEXITY AND RISK

When it comes to managing digital trust, companies today are facing increasing complexity and risk in every lane of IT. Infrastructure teams are fielding certificate renewals with shorter validity periods and changing IT infrastructures. Identity and access management teams are adopting zero-trust architectures and needing to rapidly adapt their infrastructure to support hybrid remote workforces. SecOps teams are viewing quantum computing on the horizon and thinking through how to achieve crypto-agility. This confluence of market trends is driving increased interest in digital trust as a strategic investment rather than a utilitarian backroom function.

Taking a closer look:

INFRASTRUCTURE TEAMS

Primary challenge: Preventing outages and reducing the risk of business disruption

Shorter TLS validity periods put operational stress on IT infrastructure teams. With more frequent renewals, there is increased opportunity for missed or misconfigured certificates that can lead to outages. In addition, with certificate use cases expanding, teams may not be aware of certificates being issued from other departments, which may lead to breaks in issuance policy or leave certificates driving critical business systems unmanaged.

IDENTITY AND ACCESS MANAGEMENT

Primary challenge: Securing users and devices at scale

Zero Trust architectures are transforming how organizations think about identity and authentication. These changes, based on "never trust, always verify" principles are having a profound impact on how companies secure users, devices, data, and email. These shifts are even more pronounced with more employees suddenly shifting to remote home work, yet still expecting seamless, secure access to corporate resources. In this environment, companies are searching out ways to a) improve the user experience b) simplify the IT support burden c) support more use cases d) drive corporate-wide adoption and e) improve security by eliminating time delays in provisioning or revocation.

SECOPS

Primary challenge: Crypto-agility and timely remediation of vulnerabilities

Data breaches continue to grow. SecOps teams need digital trust architectures that can rapidly adapt to new threats, newly identified vulnerabilities, or changes in cryptography or regulatory standards. With quantum computing on the horizon, companies need to invest now in strategies that will enable them to field the rapid transformation that will be needed once we enter the post-quantum computing age.

PART II

THE PROS AND CONS OF CERTIFICATE LIFECYCLE MANAGEMENT (CLM) TO DATE

With these increasing demands and risk as the backdrop, Certificate Lifecycle Management has offered the promise of centralizing visibility and control over a company's digital certificate landscape. Prior to the introduction of DigiCert(R) Trust Lifecycle Manager, companies had two choices. They could use the certificate lifecycle management offered by a Certificate Authority (CA) or designed for a particular use case (or set of use cases), or they could adopt 3rd party software that promoted the benefit of "CA-agnostic" management.

The challenge with CA-centered or use case-centered certificate management is that these systems inevitably weren't designed to cover all of a company's digital trust assets. And CA-agnostic software similarly only offered a partial solution. Many companies, when adopting CA-agnostic software, have found that they are not achieving the reliability and resiliency that comes from a more seamlessly integrated architecture. By separating the CA management from CA infrastructure, it can become difficult to identify where in the system a problem may be occurring. Further, some of the software systems were designed with a common workflow that is not flexible for the needs of different use cases, necessitating substantial investment in professional services and eventually leading to an unsustainable cost model.

These CLM systems have been a good start. But they have been insufficient. Organizations are still asking for unified, single vendor solutions that allow them to manage their full digital trust portfolio while providing the reliability and resiliency that comes with full stack operation. The ask that these organizations have is the ability to reliably manage all of the certificates across an entire organization, while addressing the unique needs of different use cases, and while reducing administrative demands and improving security. It's a big ask, and one that has not been solved by earlier CLM solutions in the market.

THE CONFLUENCE OF MARKET TRENDS IS DRIVING INCREASED INTEREST IN DIGITAL TRUST AS A STRATEGIC INVESTMENT RATHER THAN A UTILITARIAN BACKROOM FUNCTION.

RELATED RESOURCE

REDUCE THE RISK OF BUSINESS DISRUPTION

Author
Diana Jovin and Sean Crouch

Date
03-02-2023

PART III

TRANSFORMING CERTIFICATE LIFECYCLE MANAGEMENT… AND WHY WE'RE NOW CALLING IT TRUST LIFECYCLE MANAGEMENT

Trust Lifecycle Management delivers on these asks in new, value-add ways:

1. **Seamless unification of CA-agnostic certificate lifecycle management and issuance.** Why this matters: Full-stack solutions enable companies to hold one vendor accountable for the reliability and resiliency of the business systems whose operations are most critical. These solutions can be expanded to other CAs where they are needed, and expertise with CA operations ensures that these points of integration are designed by engineers who are highly skilled in PKI operations.

2. **Single pane of glass for both public and private issuance.** Why this matters: Companies are increasingly investing in digital trust as a strategic imperative, approaching the problems presented by complexity and risk with a unified strategy. To that end, solutions can no longer center on the needs of a single department or use case, and must instead provide centralized, unified management of all a company's digital trust use cases.

3. **Unified certificate lifecycle management and PKI services.** Why this matters: Systems that only provide CLM and do not offer support for the diverse technologies used by identity and access management teams, or for the workflows that govern user provisioning and revocation cycles, only address part of an organization's digital trust needs.

DigiCert Trust Lifecycle Manager, with a feature set that delivers on this promise, is the first solution to address the breadth and depth of digital trust management customers have been asking for. It is more than certificate lifecycle management. It enables companies to manage their strategic, centralized digital trust initiatives.

TRUST LIFECYCLE MANAGEMENT IS MORE THAN CERTIFICATE LIFECYCLE MANAGEMENT. IT ENABLES COMPANIES TO MANAGE THEIR STRATEGIC, CENTRALIZED DIGITAL TRUST INITIATIVES.

RELATED RESOURCE

REDUCE THE RISK OF BUSINESS DISRUPTION

PART IV

THE CAPABILITIES OF DIGICERT TRUST LIFECYCLE MANAGER

To meet today's complexity and risk challenges, a number of functions prove critical.

FEATURES FOR MANAGING CERTIFICATE LIFECYCLES

Discovery
The ability to build a centralized repository of all public and private certificates with detailed visibility and operational control.

A centralized repository, delivering the ability to continuously monitor the entire certificate landscape. This level of insight serves the entire enterprise by offering detection and visibility over every certificate, no matter where it is or what it protects. Discovery is the basis of certificate health for everything that connects, from deep within the organization to the shifting external boundaries.

Management & Notification
An alert system identifying needed actions to prevent certificate expiration or remediate vulnerabilities.

24/7/365 monitoring of all certificates, delivering the ability to reduce business disruption due to certificate expiration, vulnerabilities, or rogue activity.

Automation
Hands-free or one-touch provisioning and renewal for reducing complexity and human error.

The means to reduce complexity and error by shrinking overhead while scaling provisioning and automating manual tasks and business workflows. This includes zero-touch provisioning, pre-defined certificate templates, and access rules for compliance with security policy.

Integration
Comprehensive governance across CAs and business systems

Integration with change management, directory services, UEM/MDM, CMS, HSM, as well as technologies governing user, server, document, device, or DevOps environments. Integration tools should include customization through REST API.

FEATURES FOR PKI SERVICES

Fast CA and ICA creation
Configure for different business unit requirements

Pre-configured, customizable certificate profiles
Built for users, devices and servers

Flexible enrollment and authentication
Manual and automated methods

Integration with IAM technologies
UEM/MDM, CMS, Active Directory and more

INTEGRATION ARCHITECTURE MATTERS

Integration deserves additional attention, because it is key to execution of a digital trust strategy that addresses the many different technologies and use cases that organizations wish to support. Examples of how integration methods can play a role in use case workflows include:

Protocol support
Protocols enable organizations to leverage industry-standard methods of data exchange. Organizations depend on SCEP, EST, ACME, and CMPv2 for interfacing their certificate programs with various technologies. Protocol support enables organizations to leverage the investment that they have made in existing systems and include them in their digital trust program.

Clients
Client applications can enable organizations to address the problem of last-mile installation and automation. Many of the applications that reside on end-user workstations and laptops are customized to the unique needs of an organization. Client tools enable IT professionals to push custom installation scripts out to the organization where needed, automate last-mile installation and renewals, enforce security policy around use of MFA or password rules. By doing so, IT professionals are able to improve the end-user experience, making installation and renewal of application-centered certificates seamless and invisible to the end-user.

Gateways
Gateways support on-premises architectures where direct connection of users and servers to outside resources is prohibited. In these environments, the gateway can operate as a proxy for handling these requests in a secure manner.

Native integrations
Native integrations allow for richer, out-of-the-box capabilities that reduce the need for high touch custom PKI development. With DigiCert, pre-configured certificate templates pair with native integrations with technologies such as Intune, Windows Hello for Business or ServiceNow, eliminating the need for administrators to research and build certificate integrations.

APIs
APIs allow for the development of custom integrations, often to customer systems or to support automation strategies

For a management solution to truly address all the variation and specificity of each workflow inside a unique organization, it needs to be able to operate with dependable, flexible, and deep integrations that include native support.

TRUST LIFECYCLE MANAGEMENT IS THE NEW MODEL FOR THINKING ABOUT AND DOING CERTIFICATE MANAGEMENT.

RELATED RESOURCE

REDUCE THE RISK OF BUSINESS DISRUPTION

Author
Diana Jovin and Sean Crouch

Date
03-02-2023

CONCLUSION

TRUST LIFECYCLE MANAGEMENT—A NEW WAY TO THINK ABOUT AND MANAGE ENTERPRISE TRUST

Whether a person is the administrator worried about certificate renewal, the IAM professional worried about authentication and security gaps, or the SecOps manager concerned about remediation, everyone inside the organization who is concerned with security benefits from managing trust as a strategic initiative.

More than a simple tool or task list for managing certificates, trust lifecycle management unifies certificate lifecycle management and PKI services, protecting corporate assets, streamlining workflows, and enabling the organization to build crypto-agility. It's the new model for thinking about and doing certificate management.

"For companies that focus their efforts on digital trust—and make it a strategic imperative for the business—the benefits are notable, including ***reliable uptime, reduced risk of data compromise****, and* ***improved user trust****".*

- Jennifer Glenn, Principal Analyst at IDC, in *Digital Trust: The Foundation for Digital Freedom*

How will you put digital trust to work for your organization?
To find out more, contact sales@digicert.com.

TRUST LIFECYCLE MANAGEMENT IS THE NEW MODEL FOR THINKING ABOUT AND DOING CERTIFICATE MANAGEMENT.

RELATED RESOURCE

REDUCE THE RISK OF BUSINESS DISRUPTION