



Automation and Encryption: A Perfect Match

February 2024

Roses are red

Violets are blue

Worried about digital certificate management and security?

Carry on, we've got you!

Love is in the air, as another Valentine's Day wings in on Cupid's arrow. While it may be tempting to take five and devour a heart-shaped box of chocolates while writing bad poetry to your amour as a singing bird dips and soars over your head, it's important to remember that cybersecurity risks don't take a holiday. This includes threats to your company's critical digital certificate management workflow.

So, put aside your poems, tell the tweety bird to pipe down, and read on to learn how our solutions manage the vital end-points of your company's digital certificate processes through encryption that ensures data confidentiality and integrity. Working in parallel, our automated solutions reduce manual effort to enable faster and more accurate certificate deployment, renewal, and revocation processes. When you use our end-to-end suite, it means one less worry on your plate. Maybe you can get back to that box of chocolates sooner than you think.

PKI: Ensuring Privacy and Authenticity

To understand the importance of automation and encryption in digital certificate management lifecycles, we first need to understand the role Public Key Infrastructure (PKI) plays. PKI secures digital identities using a combination of public and private keys to create a secure data transfer environment that ensures trust between a sender and recipient. Organizations across industries, as well as governments, rely on PKI management to protect privacy and ensure the authenticity of organizational data, communications, and digital identities.

Let's look at ways you can improve security, while driving efficiency and reducing costs around your digital certificate management workflow.

Reducing Efforts and Cost Through Automation

A recent survey found that PKI automation presents significant technical, compatibility, security, and expertise challenges for a wide range of organizations. Among those challenges are:

- increased administrative work and complexity
- costs and overhead
- older or legacy systems
- frequent expirations
- security and compliance challenges

Counteracting Vulnerabilities

Automating and encrypting your digital certificate workflow counteracts today's many vulnerabilities, including but not limited to remote and hybrid working environments, through:

- **Enhanced efficiency** that reduces manual effort and enables faster and more accurate certificate deployment, renewal, and revocation processes. The result? Significant time savings and operational efficiency.
- **Improved security** that minimizes the risk of human error. The result? Certificates are correctly issued, renewed, and revoked on time. Additionally, automated monitoring and alert systems help detect and address potential vulnerabilities, bolstering overall security posture.
- **Scalability and consistency** that empowers companies to handle large-scale PKI deployments effortlessly. The result? Consistency in certificate configurations, to help eliminate security vulnerabilities.

- **Regulatory compliance** to align with industry regulations and standards. The result? Certificates are monitored, audited, and managed consistently, reducing the risk of non-compliance penalties.

Best Practice Considerations

Keep these considerations in mind when setting up your digital certificate management workflow. While not an exhaustive list, these recommendations are straightforward and can be put into practice easily.

- Develop clear certificate management policies and procedures, including; certificate issuance, renewals, and revocations
- Classify certificates based on purpose, expiration, and criticality to the business
- Define approval processes and role-based access controls
- Ensure your workflow meets regulatory compliance requirements
- Plan for scalability to accommodate a growing number of certificates

While love matches may be on a lot of minds around Valentine's Day, consider another perfect match: the security and peace of mind that comes with automating your digital certificate management workflow.