

Keep devices compliant and worries at bay.

81% of companies experienced a certificate-related outage in the past two years.¹ Digital certificates are essential for maintaining secure network communications and preventing attackers from intercepting and stealing sensitive data. But managing them can be difficult and installing them at each device is a time-consuming, multi-step and error-prone process.

Our professional services and support teams are ready and able to handle all of this for you.



ENSURE ON-TIME CERTIFICATE RENEWAL, AUTOMATICALLY.

With Xerox® Device Manager's advanced automation and our security implementation experts, we can help businesses of all shapes and sizes avoid damage, penalties and risk.

We'll track certificate expiration status, identify unknown certificates, identify which devices do not have active certificates and enhance communication security across your network. In addition, because we manage everything through a centralized cloud-enabled platform, certificates can easily be issued, revoked and renewed in seconds – regardless of where the device is.

Innovative and scalable technology. A team of experts that has your back. It's all part of our multi-layered security approach.

AT-A-GLANCE DASHBOARD KEEPS YOU IN THE KNOW.

With our unique interactive and intuitive dashboard, you can be sure your compliance standards are being implemented in alignment with your security policies. And we notify you if certificates fall outside of your policies.

So you and your team can do more and stress less.

SCALABLE FOR FLEETS OF ANY SIZE.

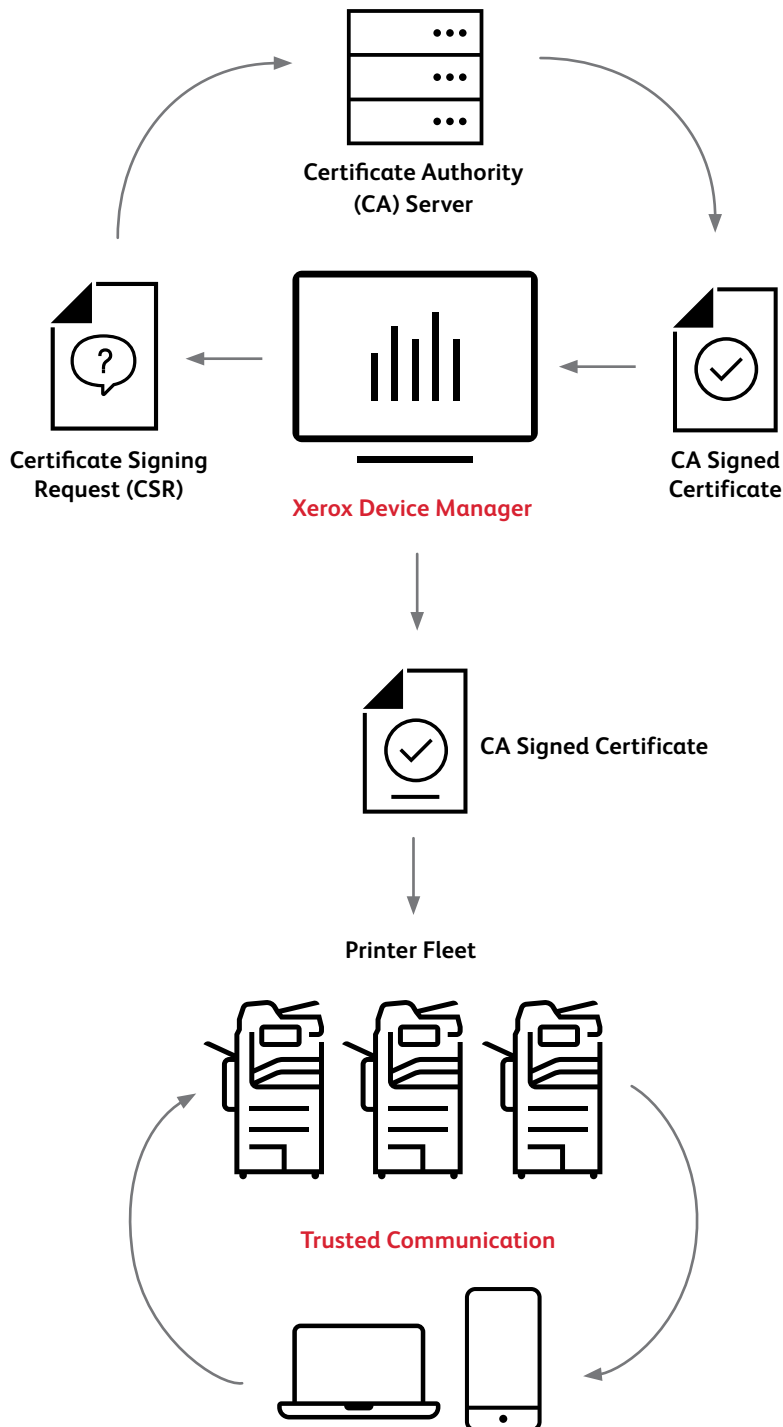
Our Device Certificate Management solution flexes for simple management of any quantity of Xerox® devices. With our technology, expertise, services and support, you gain:

- Automated and optimized creation of certificates
- Up-to-the-second and fleet-wide summaries of your certificate status
- 24/7 access to global and actionable insights
- Security compliance analytics

No matter where your printers are, we can monitor and manage them securely. You and your team won't have to do (or worry about) a thing.

¹State of Machine Identity Management Report, conducted jointly by Keyfactor and Ponemon Institute.

HOW IT ALL WORKS:



WE MAKE IT EASY TO
MANAGE DEVICE CERTIFICATES
IN ALIGNMENT WITH YOUR
SECURITY REQUIREMENTS.

This includes:

- Setting policies for certificates (either Root/Self-Signed or Trusted CA Signed)
- Obtaining and deploying original certificates, as well as renewing certificates on an established cadence
- Removing expired certificates from each device included in your policy
- Remotely remediating any non-compliant Xerox device certificates automatically to mitigate security risks and vulnerabilities
- Easy-to-access, interactive security compliance dashboards

Let us manage the lifecycle of all certificates across your network so you and your team can do more and stress less. Learn more about Device Certificate Management from Xerox at xerox.com/MPSCertificateManagement and find out about our comprehensive Managed Print Services security framework at xerox.com/mps.