intertrust

Can you afford in-house PKI for IoT?

Hidden costs and risks with in-house PKI for IoT

More than **30 billion IoT devices** are expected by **2025**.

Are you prepared to protect and manage this exponential growth?

Four questions to ask if you are maintaining certificates on your own...

1 Can you support today's short-lived certificates and multitudes of IoT devices?

2 Is your security staff up-to-date on security and regulatory requirements?

3 Is your PKI at risk due to mismanaged certificates or poor hardware security?

4 Are your PKI policies based on industry best practices or created ad hoc?

Rising concerns around PKI

66%

Understaffed

Two-thirds of enterprises don't have enough IT security staff dedicated to PKI deployment.

73%

Frail infrastructure

73% of IT professionals admit digital certificates cause unplanned outages.

60%

Slow to react

60% of organizations cannot properly detect and respond to a PKI breach.

Attacks increasing

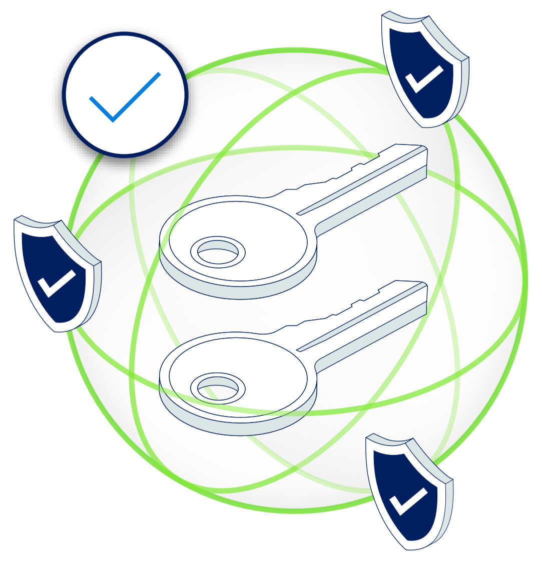
IoT cyberattacks more than doubled year-on-year during the first half of 2021.

Isn't it time to offload the burden of maintaining your own public key infrastructure?

https://www.securitymagazine.com/articles/91695-of-enterprises-not-equipped-to-respond-to-data-breaches
https://www.helpnetsecurity.com/2020/02/14/digital-certificates-downtime/
https://www.healthcareitnews.com/news/pki-mismanagement-leaves-healthcare-organizations-vulnerable
https://www.iotworldtoday.com/2021/09/17/iot-cyberattacks-escalate-in-2021-according-to-kaspersky/

A PKI service purpose-built for IoT

Streamline IoT operations with an outsourced, best-in-class PKI that reduces operational cost and risk of maintaining in-house hardware, staff, and manual PKI systems



Download the brief now