We'll dig into the more technical aspects of PKI starting in step three. But first, you'll need a high-level understanding of the risks you must mitigate in your business. Examples of these security risks include:

- Preventing unauthorized access to web services
- Preventing unauthorized access to knowledge stored in databases
- Preventing unauthorized access to your network
- Verifying authenticity of messages transferred on your network

Defining these basic risks first will help identify which can be solved using PKI.

With PKI, you can significantly increase the security level of your network. PKI binds an identity to a public key. This allows you to mitigate risks through encryption, digital signatures, and authentication. Encryption will help you mitigate risks to confidentiality. Digital signatures will help you mitigate risks to integrity. Authentication certificates will help you mitigate risks to access controls. This can be applied to various applications.

Common PKI use cases:

- Securing web pages
- Encrypting files
- Authenticating and encrypting email messages using S/MIME
- Authenticating logins using smart cards
- Authenticating nodes connecting to a wireless network
- Authenticating connections to your VPN
- Authenticating connections to sites and services containing corporate data using TLS mutual authentication

Once you identify your non-negotiable network security risks, and decide which of these can be mitigated using PKI, it's time to plan your PKI architecture.

Most mature enterprises have built a hybrid architecture that includes both public and private PKI. They typically use public PKI to secure their public-facing websites and services, and private PKI to secure their internal ones. They also differ on how automated their process is for delivering certificates.

To find the right PKI mix for your organization, you first need to identify where you need private PKI and where public PKI will be more advantageous. As promised, let's dig into some of the more technical PKI considerations.

PRIVATE VS. PUBLIC PKI

With PKI, you're binding an identity to the public key through a signing process. That signature is performed by a root, or with an intermediate that chains up to the root. Only certificates issued from roots you trust are recognized as valid.

If the root that bound the identity to the public key is in your trust store, then you can rely on the identity bound to the

public key (rely on the subject of the certificate). This is all because the certificate was issued by a root you trust.

So, what's the difference between a public root and a private root? When and how should you use each?

WHEN TO USE A PUBLIC ROOT

The technology used for signing a certificate is the same whether signing with a private or public root. Instead, the difference is that a publicly trusted root is already distributed out to browsers, operating systems, phones, etc. When a user tries to visit your site, her browser (e.g., Google Chrome,

The benefits of a private root for authentication boil down to control. Only your organization has the rights to issue certificates from your own private root. This gives you more control over the issuance process, certificate profiles, and subjects named in certificates.

Once you've identified where you need private certificates for your internal services, decide whether you should create an internal PKI (build) or use a hosted PKI service (buy).

Both build and buy are good options. The decision comes down to the resources and personnel you're able to dedicate to PKI. A hosted service creates your root and secures it at a level commensurate with public trust anchors. An internal CA gives you full control of the issuance process, but requires you to take on the costs of software, hardware, licensing, and training. We'll go into more detail about the benefits

Flexibility. Another common misconception many have is that they won't be able to accomplish the same goals with a hosted solution as they could with an internal CA. For example, you might wonder whether you can automate certificate issuance with a hosted solution. Many commercial CAs have tools, like RESTful APIs, for automating certificate management. Before you choose a commercial CA, check out its p50xte

the budget and time, and that you truly need the control and customization an internal CA provides. Keep in mind, however,

COSTS OF AN INTERNAL PRIVATE PKI

Hardware, Software, and Licensing	• CA server—included with Microsoft Certificate Services (2 recommended for redundancy) • Online Certificate Status Protocol (OCSP) and Certificate Revocation List (CRL) distributed services for redundancy, high availability, and fast response times • Firewalls and segregated networks (Firewall, switch, and dedicated rack space) • Storage mechanism for offline root and backup of offline root (HSM required) • Signing HSMs—Gemalto Luna 5 ~$40k-60k (2 recommended for redundancy)
PKI Expertise	
Training	• Regular training to keep personnel updated on latest PKI changes • Courses, certifications, and conferences
Certificate Policy (CP)/ Certificate Practices Statement (CPS)	• See most up-to-date reference (RFC 3647) for details: https://tools.ietf.org/html/rfc3647 • Writing a CP/CPS (80+ hours of work for PKI staff) • Maintaining a CP/CPS (living docs that need to be kept up-to-date) • Enforcing CP/CPS in software, policies, and rules
Auditing Against Certificate Policy	• On-going logging of key portions of PKI as evidence for audit • Yearly audit of check compliance with policies in CP/CPS
Vulnerability Testing	• PEN testing for C;9EPsMC 1.5 0 N8kF.5 (ools.ietfundancy, high a)6.3 (v)7.4 (ailability, and fast respons • ofany por •

BENEFITS OF A HOSTED PRIVATE PKI

Costs Avoided by Using a Reliable Hosted Private PKI

- Trained personnel to securely manage the CA
- Hardware, software, and licensing
- Industry updates in servers, browsers, and libraries
- High-availability and revocation infrastructure (OCSP & CRLs)
- Certificate management via API

5. Automate Certifcate Delivery

For your PKI to run smoothly at a large scale, you'll need to automate certifcate deployment. Changing industry standards and shrinking certifcate validity periods mean automation won't be an option in the future—it'll be a necessity. You might oversee 7nr.3 0 -2.55(ou might o)6.4 (C4 (C005005.le

One cost engineers often overlook is the cost of personnel. Not just the cost of hiring additional personnel to build and manage the internal CA, but the opportunity cost of your engineering team's time. If they're putting hours in to build an internal CA, they're taking hours away from their core projects.

Your engineering team has many other responsibilities for security and maintaining infrastructure—like email servers, wireless, penetration testing, audits, risk assessments, and the list goes on.

Then, the SCEP service takes it from there to get a cert on

DigiCert Cloud CA. Our hosted solution lets you keep the control with none of the maintenance frustration. We'll create your root and secure it at a level commensurate with public