

Token Migration Solution Considerations

Total Cost of Ownership Issues:

Cost containment is a focus for most organizations. In many cases, token solutions are proving to be too costly to maintain. There are substantial costs associated with:

- Maintaining the backend server infrastructure that provides token validation
- Staffing to support the solution
- Replacing lost tokens
- Recovering unreturned tokens from groups such as contractors and partners
- Maintaining and replacing token authentication devices and infrastructure



Total Cost of Ownership issues specific to software tokens include:

- Costs associated with desktop compatibility testing
- Initial deployment costs as software has to be loaded on users' machine
- Upgrade costs for new versions and renewed tokens as new deployments are necessary

The issue is how to contain and lower costs and maintain effective, high quality security.

Do your users truly need device independent roaming capabilities?

The primary advantage of hardware tokens is they provide independent roaming capabilities from device to device without the necessity of any authentication device on the PC (such as a smart card reader or USB port). Today, however, most people use their personal laptop to enter networks from different locations. In this new reality, the laptop itself can be the token, with the added benefit of being able to authenticate not just by user and password, but by individual device as well. Just as certificates today are used worldwide to identify and manage mobile phone usage, this can be extended to your corporate laptops and their users.

Certificates are a versatile, cost-effective alternative to tokens ... providing broader business value and increased operational efficiency.

While tokens are used almost exclusively for strong authentication, CERTIFICATES have many more uses:

- Secure e-mail
- Digitally sign documents and e-mails legally and recognized globally
- Encrypt data in transit and at rest on your employees laptops to prevent theft of data
- Remotely revoke certificates to shut down individual devices from entering your network(s)
- Natively integrate into most of today's leading applications to enable security beyond authentication

Today, certificates can be managed On-Demand:

- Certificate lifecycle management is a proven and established process
- PGP TrustCenter manages the backend infrastructure for the system, providing tremendous cost savings
- PGP TrustCenter customers do not need servers or as many personnel supporting the solution.

The Advantage of Working with PGP TrustCenter

PGP TrustCenter provides digital trust between employees, clients and suppliers doing business electronically through on-demand certificate management services. The company's solutions enable a wide range of digital trust applications to provide strong authentication, secure e-mail, digital signatures, data encryption and support compliance with privacy and other regulations. PGP TrustCenter was the first to provide digital certificate management through a Software as a Service model and remains the leader through its breakthrough economics, versatility and implementation speed for enterprises. Unlike traditional PKI and private certificate authority options, PGP TrustCenter solutions can be implemented in 70% less time and 70% less cost.

This document is for information only and without responsibility. PGP TrustCenter reserves the right to change scope of services.