

Top 5 One Time Password (OTP) Integration Points

Let a [leading strong authentication consultancy](#) share some of their top thoughts for integrating a one time password (OTP) solution as they understand the challenges and commonly faced issues when delivering security solutions with high availability, performance and scalability.

1. Microsoft OWA

The first step towards full remote access for many organisations is to allow employees remote access to corporate emails while out of the office. As access to Outlook Web Access (OWA) does not give a user full access to the corporate network, companies see this as a small risk and often implement without due consideration. Although not giving access to the full corporate network, giving access to emails, calendars, tasks and contacts poses a huge security risk for a company.

Although the security of the Outlook data is secured while the data is transmitted over the https protocol the weakness of a static password still exists. Imagine the effect on a business if a hacker obtained an employee's username and password and was able to access their email and send fraudulent emails or steal valuable data stored within the employee's inbox or outbox.

Integrating an one time password (OTP) solution with Internet Information Services (IIS) & OWA by enhancing the inherently secure transport layer with a second factor of authentication will greatly reduce this risk and can be implemented relatively easily.

2. Microsoft ISA/TMG

For many SME's Microsoft's ISA/TMG server is their gateway to the Internet, and once employees have been given access to their corporate email from outside the confines of the relatively 'safe' corporate network, their desire to perform more business tasks externally increases dramatically.

MS ISA server is the chosen tool for this job, but a standard installation using simple Active Directory (AD) usernames and passwords runs the same increased risks of attack from hackers as the implementation of OWA without a two factor authentication (2FA) solution.

Giving access to the corporate virtual private network (VPN), intranet and OWA through the ISA/TMG server still requires a strong authentication solution such as an OTP to strengthen the resilience to unwanted credential attacks.

3. Microsoft IAG/UAG

Microsoft's Internet Application Gateway (IAG) & Unified Access Gateway (UAG) enable large enterprises the ability to give mobile and remote workers, partners and customers, easy, flexible, and secure access to virtually any application from a broad range of devices and locations.

Opening up the corporate network in these ways further increases the risk of attack and therefore the implementation of a strong authentication solution at this level of flexibility is essential.

An OTP solution can easily be integrated with MS IAG/UAG with the use of vendor specific software agents that redirect authentication requests to the relevant OTP authentication server.

4. Citrix WI

Many businesses offer access to centrally managed applications and virtual desktops through the use of Citrix's XenApp & XenDesktop. Citrix Web Interface (CWI) provides users access to both XenApp applications & XenDesktop virtual desktops.

It is common with implementations of CWI that a user's AD username & password are used for authentication against the CWI. Again this falls far short of having a secure centralised application server, as although the method of delivering the applications and desktops is secure the authentication process is still relatively weak.

Integrating an OTP solution, that will enhance the resilience of unwanted attacks, in to the authentication process of a

SymTex specialises in Microsoft SQL server development, support and consultancy, business intelligence, .NET programming and strong authentication solutions. Clients of SymTex include big banking corporations, insurance giants and national utility companies. Symtex work nationwide located in Nuneaton, London and Leeds and specialise in supporting clients with more than 100 employees.

Top 5 One Time Password (OTP) Integration Points

Let a [leading strong authentication consultancy](#) share some of their top thoughts for integrating a one time password (OTP) solution as they understand the challenges and commonly faced issues when delivering security solutions with high availability, performance and scalability.

CWI simply requires the relevant software agent that will interact with both the CWI and the OTP server.

5. MS IAS/NPS (RADIUS)

With the majority of larger corporations using proprietary gateway and perimeter security appliances, implementation of an OTP solution cannot be integrated directly with the use of a software agent alone. These vendor specific appliances give excellent levels of functionality and network protection but still all suffer from the same risks associated with static passwords.

With the use of Microsoft's Internet Authentication Service (IAS) or Microsoft's Network Policy Server (NPS), which are Microsoft's implementations of the Remote Authentication Dial-In User Service (RADIUS), these proprietary appliances that are RADIUS client capable are able to authenticate against IAS or NPS. Both IAS & NPS have the ability to be integrated with an OTP solution.

Therefore delivering an OTP solution in conjunction with IAS or NPS and configuring the proprietary appliances accordingly allows a business to make use of existing architecture and secure their appliances functionality with an OTP. Some appliances that will benefit from implementing an OTP solution in this way include ranges from Cisco, Citrix, Juniper etc

For further help call 0800 5870 949 or find us at:

 [Subscribe to our Blog](#)

 [Follow us on Twitter](#)

 [Join us on LinkedIn](#)

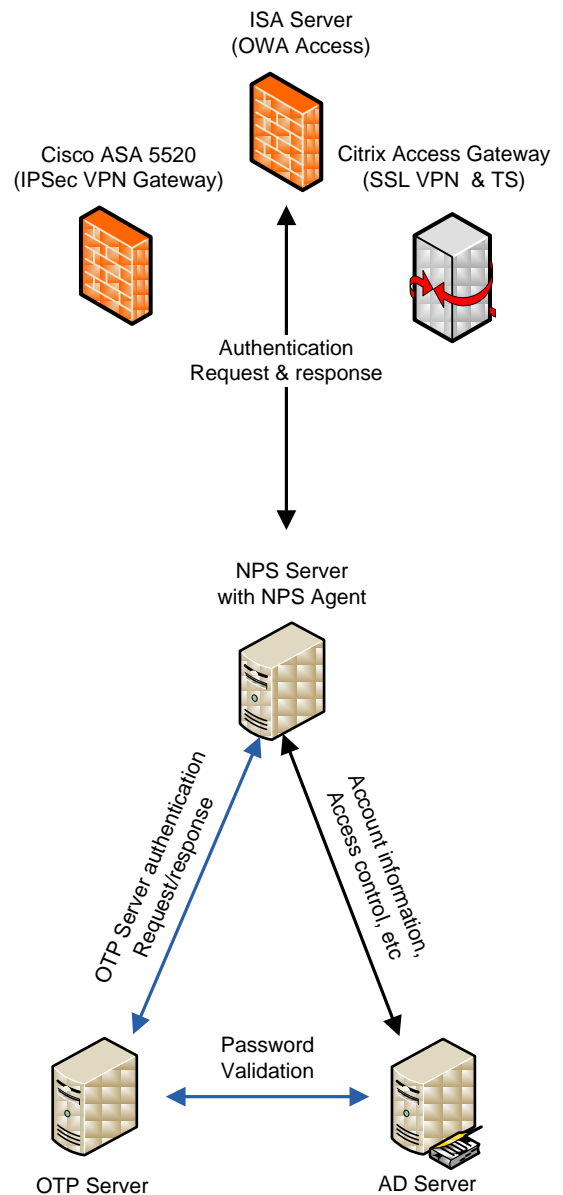


Figure 1: RADIUS based authentication model

SymTex specialises in Microsoft SQL server development, support and consultancy, business intelligence, .NET programming and strong authentication solutions. Clients of SymTex include big banking corporations, insurance giants and national utility companies. Symtex work nationwide located in Nuneaton, London and Leeds and specialise in supporting clients with more than 100 employees.