FOAS Scheme

- VPN/Terminal Server Authentication
- Citrix Authentication
- Outlook Web Access Protection
- Domain Access Protection
- Web Server (Apache/IIS) Protection
- Mobile-based Authentication
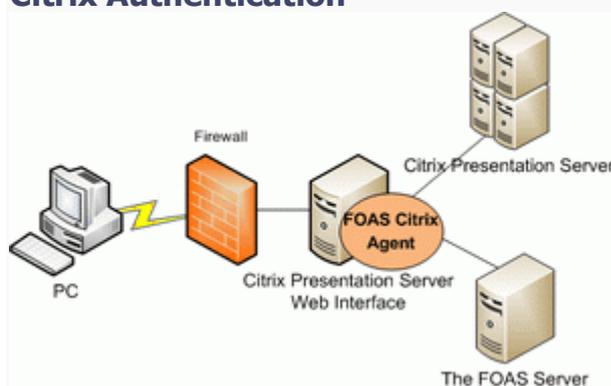- SMS Authentication
- Single Sign On

VPN/Terminal Server Authentication

Network devices (most VPN, firewalls, routers or exchange servers) support standard RADIUS protocol. Other application servers can use this solution as long as they support standard RADIUS protocol.

When an end-user wants to login, the OTP generated by the OTP token will be sent to the FOAS server through the VPN server based on standard the RADIUS protocol. The FOAS server will then return the authentication result to the VPN server, which either grants the VPN client to log in or refuses a login request.

The standard RADIUS solution is easy to employ (simply setup communication with the FOAS server on the application server) with no installation required for the FOAS agents.
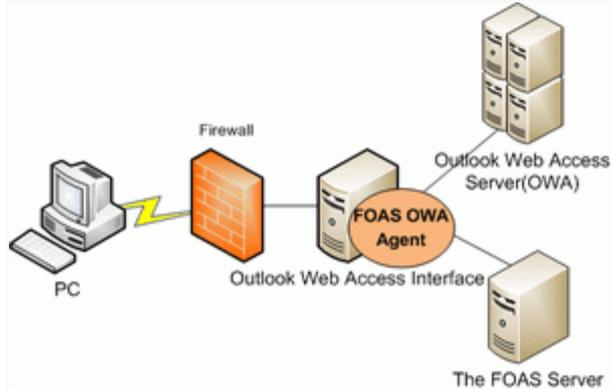
Citrix Authentication

Applications such as the Citrix Presentation Server can use the FOAS agent solution. Authentication requests are sent from the Citrix Presentation server Web Interface to the FOAS server through the FOAS Citrix agent.

When an end-user logs in, an OTP needs to be generated by the token and sent to the FOAS server through the FOAS Citrix agent at the Web Interface. The authentication result will be returned to the Citrix Presentation Server to decide whether to allow the end-user to log in.

The FOAS Citrix agent can be simply installed to seamlessly integrate with the Citrix Presentation Server Web interface so as to provide enhanced security.

Outlook Web Access Protection

Applications such as the Outlook Web Access (OWA) Server can use the FOAS agent solution. Authentication requests are sent from the OWA Interface to the FOAS server through the FOAS OWA agent.

When an end-user logs in, an OTP needs to be generated by the token and sent to the FOAS server through the FOAS OWA agent at the Web Interface. The authentication result will be returned to the OWA Server to decide whether to allow the end-user to log in.

The FOAS OWA agent can be simply installed to seamlessly integrate with the OWA Interface so as to provide enhanced security.

Domain Access Protection
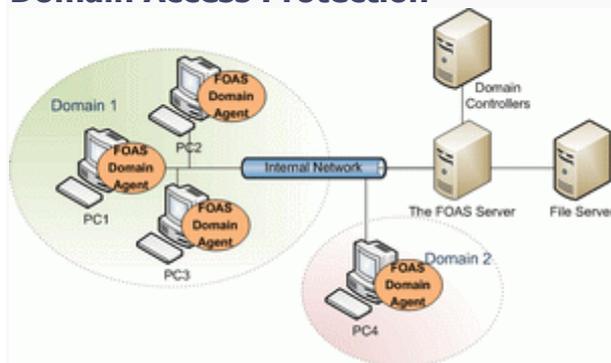
Internally, a business may wish to integrate two-factor authentication, specifically OTPs into the domain access process, where the FOAS agent solution can be used. OTP Authentication requests and normal domain authentication requests are forwarded to the FOAS Server and the domain controllers to handle respectively.

When an end-user logs in, an OTP needs to be generated by the token and input through the OTP interface provided by the FOAS domain agent. The authentication result of the FOAS server will be forwarded to the domain controller to decide whether the user is allowed to log in.

The FOAS Domain agents will need to be installed at each domain PC that needs protection.

Web Server (Apache/IIS) Protection
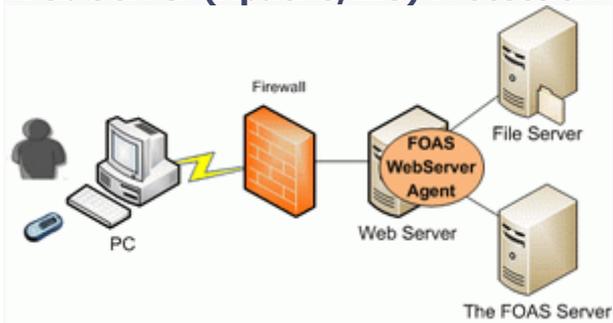
Web services such as IIS and Apache can use the FOAS agent solution. Authentication requests are sent to the FOAS server through the FOAS Web Server agents.

When an end-user logs in, an OTP needs to be generated by the token and sent to the FOAS server through the FOAS Web Server agent at the Web Server. The authentication result will be returned to the Web Server to decide whether to allow the end-user to log in.

The FOAS Web Server agents can be simply installed to seamlessly integrate with the Web Server so as to provide enhanced security.

Mobile-based Authentication
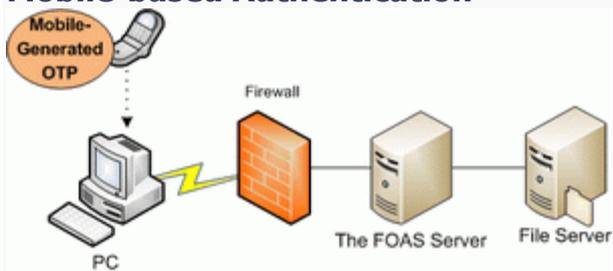
All of the above FOAS OTP Solution can be enhanced with the Mobile-based Authentication method. An OTP token is embedded into the mobile phone where a JAVA-based program will be running on the mobile phone to generate OTPs like a normal OTP token.

Similarly, when an end-user logs in, an OTP can to be generated using the mobile phone instead of a normal OTP token and sent to the FOAS server for authentication. The authentication process will be the same and the application server will decide whether the user is allowed to login or not.

There is no difference from the other solutions in terms of implementation of the FOAS system.
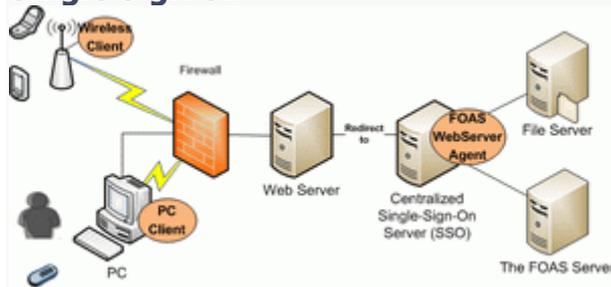
SMS Authentication
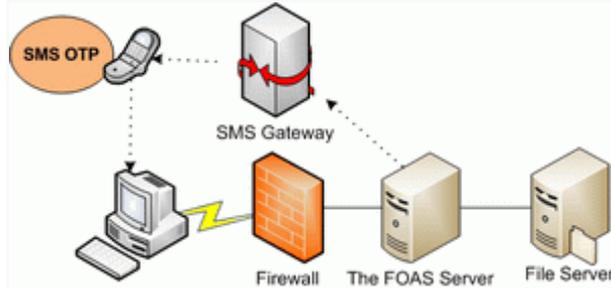
With the help of a SMS gateway, the SMS authentication solution can be introduced into the normal FOAS solutions. Authentication requests with OTPs, like normal method, will be sent through normal ways such as Internet to the FOAS server for authentication. However, the OTPs used for authentication are not generated by a normal token, but through a SMS on a mobile phone.

When an end-user logs in, a login request is sent to the FOAS server first to trigger the SMS Gateway to send a SMS with OTP to the registered mobile phone. The rest of the authentication process is unchanged.

*The deployment of the SMS Gateway may require the support from local Telecommunication providers.

Single Sign On

If a few types of OTP generators are used in the system, the Single-Sign-On solution is the best choice. Authentication requests, no matter which generation methods used, can be processed by the SSO server and sent to the FOAS server for authentication.

When an end-user logs in, an OTP can be generated by a event-based token, a time-based token, a EMV-CAP smart card reader or a mobile-based token etc. and input through the web server interface, which will be redirected to the SSO server to be further processed. The authentication result will be returned to the Web Server later to decide whether the end-user is allowed to login.