OTPDetails

Identity Provider 3.0 One Time Password Details

This page describes a one-time password (OTP) authentication mechanism for version 3 of the Identity Provider.

If you have comments/questions on the information presented here please send it to the **developer's mailing list**.

Current Thinking

Some deployments would like to have multi-factor authentication support but do not wish, or are unable, to deploy solutions like RSA SecurID tokens or client certificates because of associated cost (e.g., initial purchase, user support).

The idea behind this one time password mechanism would be to have the user authenticate with their normal username/password and then send an SMS containing a one time use code to their mobile phone. The code would then be entered on to a page displayed after the username/password login form.

An alternative to the just-in-time single use token would be to provide a mechanism for the user to request a few tokens ahead of time. These tokens would then be sent to the user's mobile phone and could be used later, for example, when the user did not have mobile phone coverage.

Additionally, for deployment to a whole community there will need to be support for user's to opt-in to such a method. User's may not be comfortable providing their mobile number to the organization or simply may not do anything sensitive enough to bother with the overhead of another step in the authentication process.

In terms of the technical details the IdP would generate the one-time use token using a secure random number generator and store the token in the IdP clustered data store. A pluggable API would be used to send the SMS. The IdP would ship with an implementation that uses the Short Message Peer-to-Peer (SMPP) protocol which is supported by the majority of SMS gateways.