

Secure CoSign Digital Signature Use via One-Time-Password (OTP) Authentication

For many organizations worldwide, secure signer authentication is an essential need. CoSign® digital signatures provide the solution for this need. This document expands on how the CoSign digital signature solution can use a One-Time-Password (OTP) for user authentication. The document also addresses various validation techniques developed for future versions of the CoSign digital signature solution.

An OTP is a constantly changing password that can be used to increase security levels and restrict user access to CoSign. OTPs are used in two-factor-authentication, which is a security system involving two unrelated elements that are used in combination for assuring the identity of the end user. Two-factor-authentication involves an OTP-generating device (e.g., an OTP hardware token or mobile phone) and another factor known to the user (e.g., a PIN code or a password). Only successful validation of both elements provides sufficient assurance of the end-user's identity. For a central server-based signature solution such as CoSign, high-level authentication of the signer is a key factor in the security of the overall system.

A fundamental component of any OTP solution is the OTP-generating device. This device is available in any of the following forms:

- 1) **OTP hardware token:** Typically, a push of a button on the token will display a unique OTP value (Figure 1).
- 2) **Applet running on a mobile phone, PC or PDA:** Managed the same way that the OTP token provides a one-time-password, except for the fact that that no hardware token is necessary because the applet program runs on a mobile phone, PC, or PDA.
- 3) **OTP via SMS text message:** The OTP is generated at a center and sent as a text message to the receiving device.



Figure 1 - OTP Hardware Token

In CoSign OTP implementations, user management and binding of the OTP tokens to users is accomplished using vendor-specific tools. CoSign uses the standard [RADIUS protocol](#) for validating the OTP values. The RADIUS protocol is a networking protocol that provides centralized authentication, authorization, and accounting management for computers.

In order to implement two-factor-authentication, the CoSign user enters their fixed password into the CoSign interface as well as their OTP. CoSign validates the fixed password with Active Directory (AD), Lightweight Directory Access Protocol (LDAP), or its internal database. The OTP value is passed as a standard RADIUS request to the vendor-specific OTP authentication server. If the results of both the fixed password authentication and the OTP authentication are successful, a signature operation will take place with the specific user's CoSign signing key.

In future versions of CoSign, ARX will use an internal self-sustained OTP validation server based on [OATH](#)¹ within the CoSign appliance. This will enable OATH-compliant software or hardware OTP tokens to be used for authentic access to the CoSign appliance.

¹ An industry standard for common algorithmic use in OTPs. OATH stands for Open Authentication.