

PRODUCT SHEET:
CA ArcotID PKI

CA ArcotID PKI Secure Software Credential

High security, high convenience

agility
made possible™



Overview

Organizations have access to a variety of strong authentication methods from which to choose. Traditionally many companies have had to resort to hardware one-time-password (OTP) tokens to achieve the desired level of security. Hardware tokens provide strong authentication but are costly and tedious to deploy, easy to lose, and must be replaced regularly. They are also more susceptible to, and do not protect against, man-in-the-middle attacks. In the past, authentication solutions fell into the category of “You get what you pay for.” They tended to be either inexpensive and simple to use, yet insecure; or they were very secure, but expensive and difficult to implement. The CA ArcotID PKI bridges the gap by delivering a strong authentication solution with both high security and high convenience.

Benefits

The CA ArcotID PKI is simple to use and eliminates the hassle and cost associated with hardware token deployment, management and distribution. You can add strong authentication to any application without changing your user’s login process. The CA ArcotID PKI delivers the strength of PKI with the simplicity of a password, making it ideal for both enterprise and consumer uses. The CA AuthMinder Versatile Authentication Server (VAS) manages the CA ArcotID PKI and also provides a wide range of authentication methods so that you can choose your authentication method based on the level of risk and your user community.

CA ArcotID PKI offers strong security and convenience to users

Hardware tokens provide strong authentication, but the cost of the tokens and the cost of deploying and distributing them can be prohibitive. There is also a higher risk with the use of OTP tokens. OTP tokens do not protect against man-in-the-middle attacks. And, as we have learned recently, if the keys to the token seed values are compromised, the tokens are rendered insecure and have to be completely replaced.

With the CA ArcotID PKI secure software credential you receive two-factor strong authentication, completely in software. No hardware tokens are necessary. You are able to add strong authentication to any application without changing your user's login process. The CA ArcotID PKI delivers the strength of PKI with the simplicity of a password, making it an attractive option for all users including employees, partners and customers.

Patented protection

CA ArcotID PKI secure software credential combines strong key protection with the low cost and simplicity of a software solution, providing strong, two factor authentication. Users can authenticate safely anytime and anywhere with the CA ArcotID PKI. The CA ArcotID PKI is based on a standard x.509v3 digital certificate, and is protected by a patented Cryptographic Camouflage™ private key concealment technology. Through this combination, the public key is encrypted with the domain key and then stored in the CA Arcot extension in the certificate. The corresponding private key is then “cryptographically camouflaged” and hidden from would be attackers to protect against brute force attacks.

Easily deployed

Since the CA ArcotID PKI is a 100% software solution that features a username/password interface, it allows organizations to replace their current authentication methods without changing the user's experience. It is completely transparent to users because they log in as they always have with their username and password, but behind the scenes the strength of PKI protects them.

Flexibility

The CA ArcotID PKI is flexible enough to work across applications and environments, and scale to millions of users. You can use the CA ArcotID PKI on any supported client device, such as a PC, notebook, PDA or mobile phone. You can also carry it on a CD, USB, or crypto token while still protecting against compromise or tampering.

Invisible to the user

The user never has to see their CA ArcotID PKI or the client that communicates with CA AuthMinder. This is especially good for consumer applications where you don't have control of the user's desktop. There are a flexible set of CA ArcotID clients to meet various deployment scenarios: JavaScript client, ActiveX native client, desktop client, Flash client, signed applet, mobile client application, mobile library and dedicated VPN client.

Each client has unique attributes and capabilities. You can choose the client type based on the needs of the application and user community. A single client is capable of handling multiple IDs issued by different organizations for different purposes. The client can also handle multiple functions including strong authentication and digital signing.

Eliminate hardware costs

The CA ArcotID PKI's software form factor makes it easy to deploy and manage. Users can self-provision their CA ArcotID PKI, eliminating the cost of token distribution and replacement.

Prevent man-in-the-middle (MITM) attacks

The CA ArcotID PKI helps protect against many common internet attacks, including Man-in-the-Middle (MITM) attacks. In order to protect businesses and customers from these attacks, CA ArcotID PKI uses a standard PKI challenge\response sequence to communicate with the CA AuthMinder authentication server protecting the online application. CA ArcotID PKI takes several steps to authenticate to the server. First the server sends a hidden “challenge” to the CA ArcotID PKI. When the user provides the correct password, the CA ArcotID PKI uses the private key to sign this “challenge” to create the corresponding “response”. Only this “response” is sent back to the authentication server for verification. The password is never sent over the channel. The CA ArcotID PKI client automatically checks the CA Arcot certificate to confirm that it is connected to the domain that issued it before signing the challenge response, automatically protecting users from MITM and other phishing attacks.

The CA ArcotID PKI also enables organizations to safely send private, encrypted electronic documents via any email channel. Organizations can now encrypt and send documents to their customers so that only the intended recipient can authenticate and open the private document.

Benefits of CA ArcotID PKI

- **No change in user behavior** – Users still use a standard password but since CA ArcotID PKI is a 100% software solution, there is no token to carry or lose, reducing the cost and complexity of physical tokens.
- **Prevents “man-in-the-middle” or “brute-force” attacks** – CA ArcotID PKI will only respond to a cryptographic challenge hidden in a web page from the domain that issued it. Because an MITM attacker intercepts and forwards web pages from a legitimate web site, the CA ArcotID PKI would detect that the web page asking for the user’s password was not the correct domain and would not authenticate the user to the application.
- **Secure roaming access** – When using a public PC, users can use a secondary authentication method to receive a temporary CA ArcotID PKI, giving the user the same secure communication they would experience at their home office. The CA ArcotID PKI stays on the system only until the user logs out.
- **Password never travels** – CA Arcot users never send their passwords ‘down the wire’. Users authenticate themselves locally on their device, and the CA ArcotID PKI responds to the cryptographic challenge without ever sending digital credentials that someone could intercept and reuse.
- **Protects access to a Digital ID** – The CA ArcotID PKI enables secure digital signing by securely storing digital IDs.

The CA Technologies advantage

The CA ArcotID PKI provides a simple and cost effective means of delivering strong authentication by eliminating hardware tokens and replacing them with a 100% software solution. Since CA ArcotID PKI is entirely software, it is very easy to deploy and manage without making any changes to the user's experience. CA ArcotID PKI protects against man-in-the-middle attacks and many other common internet attacks by using a standard PKI challenge/response sequence to communicate with the authentication server. These steps taken to authenticate to the server help protect the online application from potential internet threats. In addition to providing strong authentication, CA ArcotID PKI can also enable you to send encrypted e-documents and e-statements via email. CA ArcotID PKI delivers the strength of PKI with the simplicity of a password, making it ideal for both enterprise and consumer uses.