

Behaviors for PassFree Devices

Cheyenne Software, Inc.

Table of Contents

| | |
|---------------------------------------|---|
| Private Thumbprint Authenticator..... | 1 |
| Transferable Authenticator (CAC)..... | 1 |
| Multi-purpose Reader | 2 |
| Ad-hoc Lock..... | 2 |

Private Thumbprint Authenticator

Power on.

If ROM does not contain thumbprint signature, then create one automatically, then flash red, amber, and green light simultaneously nine times (s-i-g-n-a-t-u-r-e).

Power red light.

Transmit ready-to-receive signal (universal - contains no personal information).

Activate event loop.

When the authentication request event is activated, power amber light.

When the thumbprint event is activated, compare to stored thumbprint signature and activate match event or non-match event.

When match event is activated, power green light and transmit signed user name and public key. Wait three seconds. Power off.

When non-match event is activated, transmit authentication-failed message.

Transferable Authenticator (CAC)

Power on.

If ROM does not contain signature, then create a new one automatically, and flash red, amber, and green light simultaneously nine times (s-i-g-n-a-t-u-r-e).

Power red light.

Transmit ready-to-receive signal (universal - contains no personal information).

Activate event loop.

When the authentication request event is activated, power amber light.

When the authenticate (user presses button) event is activated, power green light and transmit signed device identifier and public key. Wait three seconds. Power off.

Multi-purpose Reader

Power on.

If ROM does not contain signature, then create a new one automatically and set a flag so the first user device to attempt authentication will automatically be accepted and assigned an administrator role.

When user requests authentication, emit power to user device.

When user device signal is received (ready-to-receive), transmit authentication request.

When authentication answer is received, activate match procedure. If match, signal approval to user (not to device). If no match, signal denial to user (not to device).

When failed authentication answer is received, signal failed authentication to user (not to device).

Ad-hoc Lock

Power on.

When master requests initialization, clear all keys and set status to accept keys.

When status is set to accept keys and a user requests to accept a key, emit power to user device, wait for device signal (ready-to-receive), transmit authentication request, wait for authentication answer, and accept the public key in the answer into the electronic key ring.

When master requests end initialization, set status to not accept new keys.

When user requests authentication, emit power to user device.

When user device signal is received (ready-to-receive), transmit authentication request.

When authentication answer is received, activate match procedure. If match, signal approval to user (not to device). If no match, signal denial to user (not to device).

When failed authentication answer is received, signal failed authentication to user (not to device).

For more information about improved electronic access control using PassFree, contact:

Cheyenne Software, Inc.
(800) 935-9637
someone@mypassfree.com