

GETTING STARTED WITH CAC PIN RESET (CPR)

The CAC PIN Reset Workstation (CPR-WS) application was designed by the Defense Manpower Data Center (DMDC) to provide DoD organizations with a secure and convenient CAC PIN reset capability. CPR-WS uses off-the-shelf hardware to enable CAC PIN's to be reset locally by designated CPR Trusted Agent Security Managers (TASM's) and CPR Trusted Agents (CTA's). The availability of CPR-WS can negate the need for an individual to physically report to a CAC issuance facility to have their PIN reset by a RAPIDS workstation. The use of CPR-WS at a local command can help prevent inconvenience and lost productivity for the CAC holder, and can also help to ensure that RAPIDS workstation utilization is more focused on CAC and ID card production needs than on PIN resets. Additionally, RAPIDS workstations at CAC and ID card issuance facilities are not staffed to provide PIN resets on a 24/7 basis. CPR-WS was developed to provide DoD components with a readily available, cost effective, and flexible solution to the problem of "locked" CAC's.

CPR-WS hardware is comprised of a laptop or desktop personal computer, a 4-port USB hub, a fingerprint reader, two CAC readers, a PIN pad, and a mouse. CPR-WS requires network connectivity, which can be provided by legacy networks, ONE-NET, the Navy and Marine Corps Intranet (NMCI) via a Contract Line Item Number (CLIN) 6AR "wall plug," or through a commercial internet connection. The CAC PMO is currently working to develop a specialized CPR "seat" for NMCI. Once implemented, the NMCI CPR seat will enable sites to order a complete CPR workstation package (including network connectivity) as a single CLIN from the NMCI Electronic Marketplace. In the interim sites wishing to utilize NMCI for CPR connectivity must continue to procure their own CPR workstation hardware and must order the CLIN's required for the NMCI wall plug through their local ACTR. Please contact the CPR Project Officer at the CAC PMO for more information on how to obtain a NMCI CLIN 6AR wall plug. Please note that CPR-WS application software cannot be installed on a standard NMCI workstation seat.

New CPR sites must first designate a primary and an alternate Trusted Agent Security Manager (TASM) to manage both the CPR workstation(s) and any CPR Trusted Agents (CTA's) assigned to their site. The *CPR User's Manual and Business Policy Statement* contains detailed information regarding the TASM's functions and responsibilities. CPR sites must register their primary and alternate TASM's by forwarding three required forms to the CPR Project Officer at the CAC PMO via email. These three forms are: **1.) CPR TASM Registration/Revocation Request Form (modified DD Form 2875); 2.) CPR User Qualifications Affidavit; and 3.) TASM & CTA Acknowledgement of Responsibilities form.** The forms can be downloaded from the CPR Community Page on Navy Knowledge Online (NKO), and can also be downloaded from the CAC PMO website (links provided at the end of this document.) After reviewing and approving the submitted TASM forms, the CPR Project Officer forwards the forms to the DMDC Security Team for CPR Site ID assignment and TASM account creation. It normally takes 24 to 48 hours after the forms are submitted to the CAC PMO for the new site ID and new TASM accounts to be activated by DMDC. New TASM's and CTA's should review the documents contained in the

“CPR Training and Resources” sections of the NKO CPR Community Page and the CPR Page on the CAC PMO Website before using CPR-WS.

CPR TASM accounts are provisioned by DMDC to enable TASM’s to operate CPR-WS to reset CAC PIN’s and also to create CPR Trusted Agent (CTA) accounts for their particular sites. CTA accounts are established by the site’s TASM’s through use of DMDC’s “Security Online” web application. CTA’s are able to operate CPR –WS to reset CAC PIN’s, but cannot establish new CTA accounts. Prospective CTA’s must also complete the three CPR forms referenced in the preceding paragraph and submit the forms to their TASM’s. However, the original forms are maintained in the site’s local files, and only a copy of the “TASM & CTA Acknowledgement of Responsibilities” form is forwarded to the CPR Project Officer at the CAC PMO. Detailed instructions on the use the Security Online web application are contained in the “CPR Training and Resources” documents maintained on the NKO CPR Community Page and the CAC PMO website.

CPR-WS functions by establishing a secure channel between the CPR-WS operator’s CAC, the PIN reset customer’s CAC, and designated servers at DMDC using the Secure Sockets Layer Version 3 (SSLv3) protocol. The identity of the CPR-WS operator (TASM or CTA) is verified by DMDC during CPR-WS logon by matching the operator’s CAC, PIN, and fingerprint biometrics. The identity of the CPR-WS customer is verified by DMDC by fingerprint biometric matching and is visually confirmed by the CPR-WS operator when the customer’s digital photograph is retrieved from the DEERS database and displayed on the CPR-WS desktop. The entire CPR-WS PIN reset process from TASM/CTA logon to customer PIN reset should normally take less than five minutes. However, bandwidth constraints, DMDC server-side issues, and difficulty matching the customer’s fingerprint biometrics can sometimes slow the CAC PIN reset process. In instances in which either the customer’s identity cannot be definitively established by the TASM/CTA or the customer’s biometrics cannot be matched by the CPR workstation the customer should be directed to a RAPIDS workstation at a CAC issuance site for further assistance.

Links

Navy CAC PMO public website’s CPR Page:

http://cnic.navy.mil/CNIC_HQ_Site/WhatWeDo/AdministrativeServices/CommonAccessCardProgram/CACPINReset/index.htm

Navy Knowledge Online (NKO): <https://wwwa.nko.navy.mil/portal/home/>