



## Questions? Need More Info?

Contact the following:



**USAREUR G6**

**(AEIM-I)**

**Unit 29351**

**APO AE 09014-9351**

**Military: 314-537-6211**

**Civilian: 011-49-(0)611-143-537-6211**

**E-mail:**

***usarmy.wiesbaden.usareur.mbx.g6-ia-ppt-branch@mail.mil***



**<https://intranet.eur.army.mil/hq/iassure/>**

**Trusted Agent 24x7 Customer Service:**

**Civilian: 703-545-9450**

This publication is available at

**<https://aepubs.army.mil>**

**AE MISC PUB 25-2C • 18 JUL 16**

## IDENTITY MANAGEMENT TOKENS

(Common Access Card, Alternate Smart Card Logon, Secret Internet Protocol Router (SIPR) Token, and SIPR Administrator Token)



**Headquarters  
United States Army Europe  
Wiesbaden, Germany**

**Headquarters  
United States Army Installation  
Management Command, Europe Region  
Sembach, Germany**

## **Types of Public Key Infrastructure (PKI) Tokens: Common Access Card (CAC), Alternate Smart Card Logon (ASCL), SIPR Token, SIPR Administrator (Admin) Token**

**CAC:** The CAC is a “smart” ID card for Regular Army military personnel, selected Reserve personnel, DOD civilian employees, and eligible contractor personnel.

**ASCL:** Privileged users of the non-secure Internet protocol router network (NIPRNET) must have an ASCL token and an active personal identification number (PIN) before the privileged account will be enabled. Users who are not authorized a CAC may still be eligible to receive ASCL tokens for authentication to the NIPRNET.

**SIPR Token:** This is a hardware token that is issued to facilitate PKI authentication for the SIPR network (SIPRNET). Before any SIPR user account is created, the user must have a SIPR token and an associated PIN to log onto the SIPRNET.

**SIPR Admin Token:** SIPRNET privileged users must have a SIPR Admin Token and an active PIN before the privileged account will be enabled.

## **Background**

DOD PKI has strengthened the overall security posture in the DOD NIPR and SIPR information network environments.



## **User Information**

To obtain a SIPR token, users must—

- Apply for the token through their unit trusted agent (TA), who will verify the end user face to face. Users should contact their local information systems security manager (ISSM) and information systems security officer (ISSO) or refer to iAssure for their TA.
- Fill out DD Form 2842, Department of Defense (DOD) Public Key Infrastructure (PKI) Certificate of Acceptance and Acknowledgement of Responsibilities, and send the form and a memorandum signed by the requester’s commander or staff principal endorsing the request to the USAREUR G6 (AEIM-I).

**NOTE:** Users must return their tokens to their TA when departing the command.

## **Frequently Asked Questions**

### **What does the SIPR token look like?**

The token looks like a CAC without a photograph. It has two symbols and an embedded subscriber identity module (SIM) chip.

### **What happens to my SIPR token when I leave the unit?**

TAs will recover SIPR tokens from departing users as part of outprocessing.

### **How should the SIPR token be handled?**

The SIPR token itself is unclassified, even with the SIPR certificate loaded on it. The token is to be protected as a high-value unclassified item when not in a card reader.

### **What happens if I insert my SIPR token into an unclassified computer?**

Users should try to avoid this. Users who enter their PIN commit a security violation and their token must be revoked. If the PIN is not entered, no security violation will occur.

### **How long are SIPR tokens valid?**

Tokens and PINs are valid for up to 3 years.

## **United States Army Europe**

Contact your local Trusted Agent if any issue concerning your SIPR token arises.