

DSCA ECA Certificate: End-User Playbook v1.1

1. Overview

Welcome, valued mission partner! As part of the U.S. Department of War's modernization, your legacy RSA token is being replaced by a secure **External Certificate Authority (ECA) Certificate**. This digital credential is required to access the Security Cooperation Information Portal (SCIP) and other DoW systems.

Please read the entire document before starting this process.

2. The Onboarding Process

The entire process begins with your local U.S. point of contact, the **Authorized DoW Employee (ADE)**. This is typically a Security Cooperation Officer (SCO) at your local U.S. Embassy.

Phase 1: Requesting Your Voucher

1. **Identify Your ADE:** Your first step is to identify your designated local Authorized DoW Employee (ADE). A continuously updated list of approved ADEs, organized by country, is maintained on the public SCIP portal.
 - **Action:** Navigate to <https://scip.dsca.mil/> to find the list of names and contact information for the U.S. Security Cooperation Officer (SCO) or other ADE officials assigned to your country.
2. **Contact Your ADE:** Reach out to your designated ADE to request your transition to an ECA certificate.
3. **ADE Submits Request:** The ADE will work with you to determine your technical needs (Soft Certificate vs. Hard Token) and will submit an ECA Voucher Request Form to DSCA on your behalf.
4. **Complete Online Application:** Once the request is approved, you will receive an email from Identrust containing two critical items:
 - Your prepaid **Voucher Code**.
 - A **link** that says 'Redeem Voucher' to start the Identrust Application Process:

Your IdenTrust Certificate Voucher Has Arrived

Hello ,

You have been assigned a voucher to purchase an IdenTrust certificate.

Select the button below and paste your voucher number into the voucher field to begin your application.

Voucher Information

Voucher Number:

Type:

Issuance Type: Initial Issuance

Expiration Date: 28 Jul 2027

Redeem voucher

- **Action:** Immediately use the 'Redeem Voucher' link provided in the email to begin your online application and follow the attached IdenTrust ECA Application User Guide:



IdenTrust ECA
Application User Gu

- **Note:** If you have not received an email from IdenTrust within 5 business days and you checked your junk box, reach out to your ADE and let them know. IdenTrust emails could be blocked by your email provider. In those cases, you will access the following link to redeem a voucher code that your ADE can get from DSCA: [Simplify Voucher Management - All in One Place](#)

Already Have a Voucher?

Enter Voucher Number

Redeem Voucher

- **Application Verification:** After you have completed the application, you will receive a follow-up email asking you to verify your email address and that you are the one who submitted an application or online registration. Follow the instructions of that email to verify. This is what that email looks like:

Dear

Thank you for applying for an IdenTrust digital certificate! You are receiving this e-mail as part of the verification process for your application. By following the steps below to verify your email address, you also confirm that you are the human subscriber who completed the online registration and provided the required information for the digital certificate.

VERIFICATION CODE:

1. Go to: <http://www.identrust.com/verify>
2. Enter the verification code listed above. Make sure there are no spaces before or after the code.
3. Enter the Account Password you created during the application process.
Note: If you did not record or have forgotten the password you created, you will be given the opportunity to decline the application at the link above. You will need to reapply for a new certificate as IdenTrust does not have access to view, confirm, or reset any of your personal login information.
4. Click 'Next' to complete the verification process. This e-mail verification must be completed before we can start processing your application.

Did you know? You can check your application status anytime by logging into the [Certificate Management Center](#) with your account number and application password. You may also find those instructions [here](#).

You may contact IdenTrust Customer Support with any questions by submitting a ticket via our [Customer Support Ticket Portal](#). Be sure to list your Application ID or Account number in the email.

APPLICATION ID:

ACCOUNT NUMBER:

Note: You will not receive a payment receipt until the application has been approved.

Phase 2: In-Person Identity Vetting

1. **Print Your Forms:** At the end of the online application, print the "**Part 2: In-person Identification Form.**" **Do not sign it yet.**
2. **Schedule Vetting Meeting:** Schedule a brief, in-person meeting with your ADE.
3. **Attend the Meeting:** You **must** bring the following to the meeting:
 - The **unsigned Part 2** form you just printed.
 - The pre-signed **Part 1** form you received from DSCA.
 - Your valid, unexpired **National Passport**.
4. **Sign the Form:** In the physical presence of the ADE, you will "wet-sign" the Part 2 form. The ADE will then complete and sign their section.

Phase 3: Final Approval & Certificate Retrieval

1. **ADE Digital Submission:** To ensure rapid processing, your ADE will immediately scan both documents (Part 1 and Part 2) and email them directly to IdenTrust using their CAC-signed email.
 - *Note: Your ADE will retain the original physical forms and mail them to IdenTrust or DSCA on your behalf to satisfy auditing requirements.*

2. **IdenTrust Approval:** You will receive an email from IdenTrust once your application is approved.
3. **Affiliation & Installation:** Visit section 4 of this document and install your Soft Certificate or to set up your new Hard Token. If you have been issued a Hard Token (Smart Card), you will need a **compatible USB smart card reader**. You are not required to use a specific brand or model. Any modern, TAA-compliant smart card reader that supports the PC/SC standard will work. Many users may already have a compatible reader used for other national ID card programs.

Phase 4: DoW Identity Registration (DMDC Mission Partner Portal)

Purpose: Once your ECA certificate is issued and installed, you must register it in the Department of War (DoW) central identity system to create your DoW digital identity.

Prerequisites: Ensure your Hardware Token (smart card) is plugged into your card reader, or your Software Certificate is installed in your browser, before navigating to the portal.

Step 1: Access the Portal & Initial Consent

1. Navigate to the **DMDC Mission Partner Registration Portal**:
<https://mpartnerregweb.dmdc.osd.mil/mpartnerregweb/app/>
2. **Certificate Prompt (if applicable):** If prompted by your browser, select your **IdenTrust ECA certificate** and enter your PIN.
3. **DoD Notice & Consent:** Read the standard mandatory DoD Notice and Consent banner and click "**Accept**".

Step 2: Select Credential Registration

1. On the main page, click the button labeled "**Register an approved non-DoD credential**".
2. **Certificate Prompt:** Select your IdenTrust ECA certificate from the prompt and enter your PIN if requested.
3. **Second Consent Banner:** Click "**Accept**" on the follow-up consent splash page.

Step 3: Credential Identification

- On the Credential Identification screen, click "**PKI Login**".

Step 4: Registration Application – Identity Information

1. Complete all **mandatory fields** marked with an **asterisk (*)**.
2. **Mission Partner Dropdown:** Select **IdenTrust**.
3. **Affiliation to Mission Partner:** If prompted, select Contractor.
4. Click "**Next**".

Step 5: Sponsor Information

1. In the "Your Sponsor Information" field, enter the official DoW email address of your designated sponsor:
 - **Option A (Preferred):** The full .mil email address of the designated SCIP Application Information Owner (e.g., your WebRoR sponsor).
 - **Option B:** Any authorized U.S. Government civilian, military member, or contractor holding an active DoW CAC (including your local ADE, if they are willing/authorized to act as your sponsor).
2. Click "**Next**".

Step 6: Review & Submit

1. **Review** all displayed identity and sponsor information for accuracy.
2. Click "**Submit**".
3. Confirmation: Upon successful submission, you will see an Application Confirmation screen displaying your unique Confirmation Number.
4. Click "**Exit**" to close the session.

Step 7: Sponsorship Approval & Identity Creation Timeline

- **Sponsor Action:** Your designated sponsor will automatically receive an email notification directing them to the DMDC Sponsorship Portal to review and approve your registration.
- **Processing Window:** Once your sponsor clicks "Approve", it takes between 8 to 48 hours for the DoW identity linked to your ECA to replicate across the enterprise.

Step 8: Final System Authorization (SailPoint Role Requests)

Important Reminder: DMDC sponsorship only establishes your Authentication (Identity). It does not grant application access.

Once the 8–48 hour replication window has passed, you must request your application permissions:

1. **Navigate to SailPoint - Public:**

<https://public.dod-e-icam.mil/identityiq/home.jsf>

2. Authenticate using your IdenTrust ECA certificate and PIN.
3. Submit an online system access request for your required SCIP application roles (refer to your specific SCIP application onboarding instructions for required role names).

3. Support

For any technical issues with the IdenTrust website or certificate installation, please contact the IdenTrust Help Desk. For questions about the DSCA process, please contact your local ADE.

4. ECA Certificate Install

Please use the corresponding detailed guides accordingly:

ECA Hard Certificate:



DSCA ECA
Hardware Activation

ECA Soft Certificate:



DSCA ECA Software
Activation Guide v1.