Logistics Modernization Program
Total Asset Visibility – Contractor (TAV-C)
Portal End-User Access Procedures

Change 1: adding computer specifications to access the portal. (Page 2)

LMP's TAV-C capability extends asset visibility to contractor locations, contributes to bettering the Army's view of assets, and supports Army Readiness.

FINAL Staffing Draft

Table of Contents

Introduction 2
Purpose Statement 2
TAV-C Portal End User Access Process Flow 3
TAV-C Portal End User Access Process Steps 4
Appendix A – Instructions for Online DoD ECA Soft Certificate (IdenTrust) 7
For Example Only 7
Instructions for DoD ECA Certificate Application (IdenTrust) 7
- **The production inactivity lockout period is 35 days** - If a TAV-C Portal User does not transaction in the TAV-C portal within 35 days, their Production account will become locked, which would prohibit them from using the TAVC portal transactions. 7

Help Resources from IdentTrust 8
Appendix B – TAV-C Portal User Role to Training Course Matrix 24
Appendix C – Sample DoD ECA Forms Packet 25
Appendix D – Acronym List 26

FINAL Staffing Draft

Introduction

Logistics Modernization Program's (LMP) Total Asset Visibility – Contractor (TAV-C) capability was developed to resolve audit findings related to the management of Army property. TAV-C capability extends asset visibility into contractor locations through improved record-keeping and provides more accurate records and reports associated with this Government property. Use of TAV-C functionality by contractors is mandatory for Army Working Capital Fund managed property in the possession of contractors. This solution contributes to the management of assets supporting global equipment Readiness through LMP.

Contractors using the TAV-C Portal to input information into LMP will comply with the access processes described in this guide to establish and maintain user accounts, complete access processes, as well as Department of Defense (DoD) approved authentication, to receive access to this capability. The approved authentication is achieved one of two ways: with a Common Access Card (CAC) or via a DoD External Certification Authority (ECA) issued certificate. The DoD ECA program supports the issuance of DoD-approved certificates to industry partners and other external entities and organizations. The ECA program is designed to provide the mechanism for these entities to securely communicate with the DoD and authenticate to DoD information systems.[1]

It is recommended Contractors carefully review this document and consider the amount of time needed to establish and maintain user security credentials, complete mandatory systems access training, apply for access to the system, and complete task specific user training.

— Until these requirements are satisfied, portal access will not be granted. —

Refer to Appendix B for a list of user functional training courses and refer to the solicitation to verify the TAV-C functions needed for the effort.

Purpose Statement

The purpose of this document is to provide an understanding of the process for gaining access to the LMP TAV-C Portal solution for TAV-C Portal Contractors. The TAV-C Portal Contractors include:

1) Stock, Store and Issue Contractor Portal Users, and

2) Vendor Proof of Delivery Contractor Portal Users

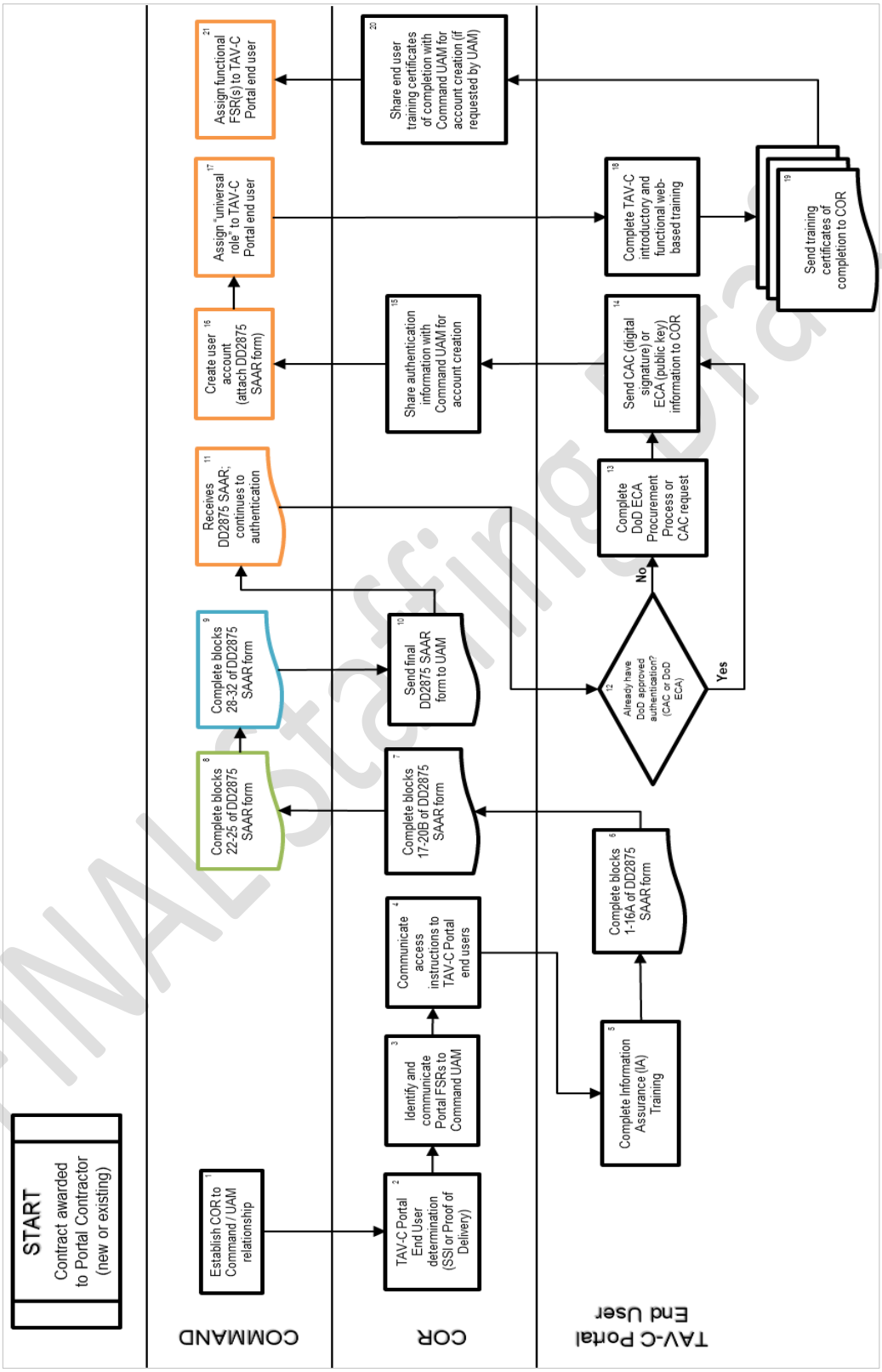
Please note that the DoD ECA process described in this document uses examples of DoD ECA issued certificates through IdentTrust. There are other providers.

Internet Access to the LMP TAV-C Portal has been validated using Windows 10, Internet Explorer 11, and Google Chrome browsers. Hardware requirements for LMP TAV-C Portal would be any hardware that can support Windows 10, Internet Explorer 11, and Google Chrome and connect to the Internet.

[1] https://www.identrust.com/certificates/dod-eca-programs

FINAL Staffing Draft

TAV-C Portal End User Access Process Flow



FINAL Staging Draft

TAV-C Portal End User Access Process Steps

- In accordance with AMC Operations Order 19-229, dated 111810Z Sep 2019, this guide establishes procedures and guidance for users to gain access to the TAV-C Portal.
- The Contracting Officer (KO) works with the requiring organization to establish a Contract Officer's Representative (COR).
- The designated COR informs the TAV-C Portal contractor of these procedures and requirements and assists end users with gaining access to the TAV-C Portal. The COR reviews and approves the establishment of LMP end user accounts supporting TAV-C Portal processes. The COR functions as the Contractor's point of contact for LMP systems issues.
- The COR works with the designated Command UAM Administrator to identify TAV-C Portal Functional Security Roles required by the contractor.

The following key requirements must be met by the TAV-C Portal end user to receive access. This section will review these requirements in greater detail.

- ☐ Information Assurance / Cyber Awareness (IA/CA) Training
- ☐ DD 2875 – System Authorization Access Request (SAAR)
- ☐ Approved DoD Authentication: Common Access Card (CAC) or DoD External Certification Authority (ECA) issued certificate
- ☐ TAV-C Portal Functional Training

Information Assurance / Cyber Awareness (IA/CA) Training–

***Note** the # refers to the process flow on page 3*

- **#5, TAV-C Portal end user** will complete the IA/CA Training Course → IA/CA training must be completed prior to submitting the DD 2875 System Authorization Access Request (SAAR) – (see step #6) to produce certificates for the COR. IA/CA training can be accessed at:
  - For CAC-enabled users: https://cs.signal.army.mil
  - For Non-CAC enabled users: https://public.cyber.mil/training/cyber-awareness-challenge-2019/

Steps 6-11 are needed to complete a DD 2875 – System Authorization Access Request (SAAR)

- **#6, TAV-C Portal end user** completes blocks 1 through 16A of the SAAR and submit to the COR.
- **#7, COR** completes blocks 17-20B and submits to responsible **Information Assurance (IA) Officer.**
- **#8, IA Officer** completes blocks 22-25 and submits to the responsible Security Manager.

FINAL Staffing Draft

- **#9, Responsible Security Manager** completes blocks 28-32 & submits to the COR.
- **#10, COR** provides a copy of the completed SAAR form to the UAM for auditability purposes.
- **#11, Site UAMs** receive the completed SAAR form and add it to the user's LMP account once the account is created (step #16).

Approved DoD Authentication

- **#4, COR** verifies a DoD External Certification Authority (ECA) issued certificate is required and is available from on-line providers.
- **#12,** If the **TAV-C Portal end user** has a DoD CAC or ECA, skip step 12 for completing the DoD ECA Soft Certificate procurement process
- **#13, TAV-C Portal end user** completes the DoD ECA Soft Certificate procurement process through an issuing company (the example contained in this document comes from the IdenTrust[2] website and is for reference only. Other ECA providers are available).
  - Follow instructions on the Contractor's selected DoD ECA provider website
  - Must be completed within **30 days from the date of the signature on the forms packet** (*instructions provided within the forms packet*)
  - **TAV-C Portal end user** will be notified by the issuing company that their DoD ECA Soft Certificate is available for retrieval, upon completion of forms processing
  - **TAV-C Portal end user** downloads DoD ECA Soft Certificate to their certificate store
    - This may require Administrator permissions on the personal computer (PC), therefore the end user may need to contact their local IT support.
    - DoD policy states that the user must enable strong encryption of their certificates. Password protection is required and begins when obtaining the certificate from the DoD ECA vendor.
    - It is recommended users complete the "Friendly Name" field with their ECA Provider for their certificate (otherwise, this will be left blank).
- **#14-16, TAV-C Portal end user** provides required information to the **COR** to be communicated to the **site's responsible UAM** for account creation and record keeping, (i.e.: public key from soft certificate or digital signature, DD2875, etc.). The UAM will verify CAC users have an existing DISA account, and non-CAC users have a valid DoD ECA certificate (Public Key).

FINAL Staffing Draft

[2] https://www.identrust.com/

Additional Prerequisite Access Requirements

- **#17, Responsible UAM** grants the TAV-C Portal end user a “universal role” to allow access to the TAV-C Training Library via the TAV-C Portal
- **#18-19, ALL TAV-C Portal end users** must complete appropriate introductory TAV-C web-based training courses. Refer to Appendix B: TAV-C Portal User Role to Training Course Matrix for further guidance.
- **#18-19, TAV-C Portal end users** must successfully complete the associated functional training courses for the Portal access that they are requesting prior to that access being provided
  - Approved authentication (via CAC or ECA) must be obtained to access the TAV-C Portal Training Material on the Portal page
  - Refer to the TAV-C Portal User Role to Training Course Matrix at Appendix B
- **#20-21, Organizations** will follow their documented policy for assigning Functional Security Roles (FSR) to Portal end users. Steps 20-21 will be completed by the requiring activity.

FINAL Staffing Draft

Appendix A – Instructions for Online DoD ECA Soft Certificate (IdenTrust)

For Example Only

Instructions for DoD ECA Certificate Application (IdenTrust)

Follow these steps to apply for the DoD ECA Soft Certificate through IdenTrust's online application.

IMPORTANT NOTE: When applying for an ECA certificate, when prompted, the **Program** is referring to "LMP – Logistics Modernization Program". The **Organization Affiliation** refers to the vendor / company you work for.

Upon submission of the application, you will be prompted to download the IdentTrust DoD ECA Forms Packet; follow these steps:

1. Verify information on page 3 of the forms packet
2. Fill out Part 2 on Page 6 (i.e.: a passport and driver's license are commonly used)
3. If you have more than one citizenship you have to assert on Page 7
4. Receive notarization on page 6, and page 7 if applicable
5. Send the completed, notarized forms packet to your Organization Officer (a Vendor point of contact) to be signed
6. Return the completed, signed, notarized forms packet back to IdentTrust **immediately**

Reminder, all processing steps must be completed within 30 days of the date the forms packet is signed

Responsibility of Certificates and User Accounts

- **Organization UAM** will manage the required annual account review, which is required for **TAV-C Portal end users**
- **Changes to Vendor End User Accounts**
  - COR and Organization UAM should follow the AMC HQ UAM Policy to handle end user account changes, account deletion, and inactive accounts, where possible
  - For any scenarios not covered in the AMC HQ UAM Policy, the COR and Organization UAM will identify a process to handle end user account changes, account deletion, and inactive accounts
  - Organization (Vendor) is responsible for notifying the Organization UAM if any LMP TAV-C Portal user no longer requires an account (i.e.: employee termination)
  - Organization (Vendor) is responsible for ensuring the Organization UAM has relevant and up-to-date information for End Users (i.e.: personnel information, certificate renewals, public keys, etc.)
    - TAV-C Portal User Accounts are subject to LMP lock out policies, as follows: The overall LMP inactivity lockout period is 45 days - if a TAV-C Portal Users does not log-in to the portal within 45 days, their account will be completely locked and their LMP account will become inactive
    - The production inactivity lockout period is 35 days - If a TAV-C Portal User does not transaction in the TAV-C portal within 35 days, their Production account will

FINAL Staffing Draft

become locked, which would prohibit them from using the TAVC portal transactions.

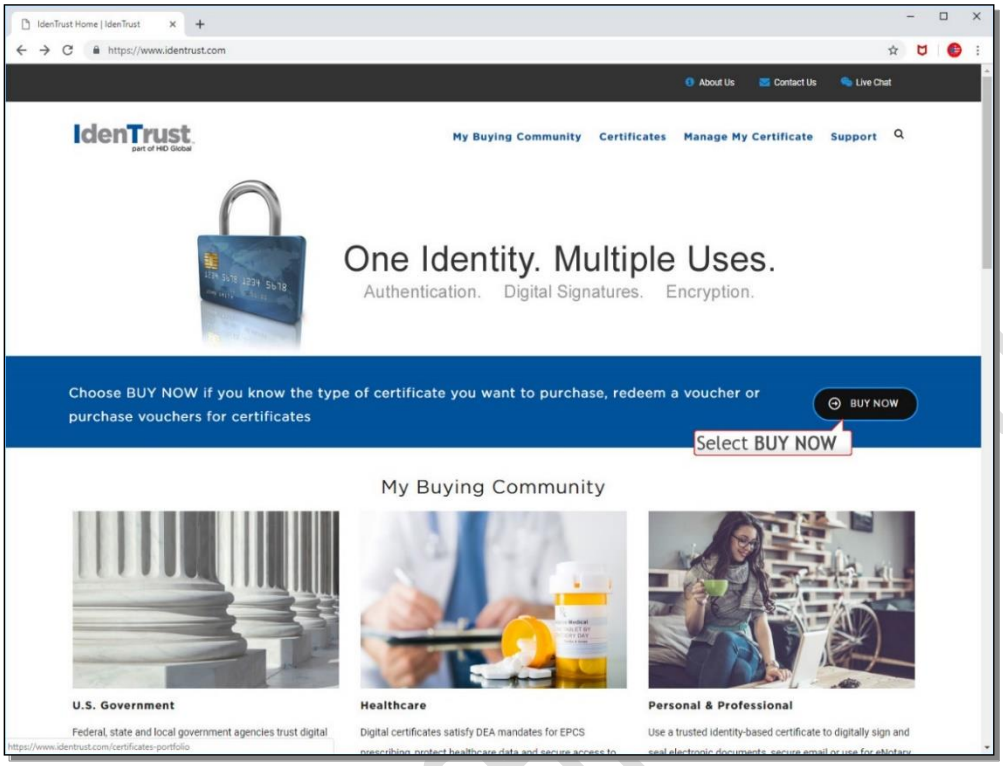
Help Resources from IdentTrust

IdentTrust offers a large library of help support documents and articles on their website, some topics include:

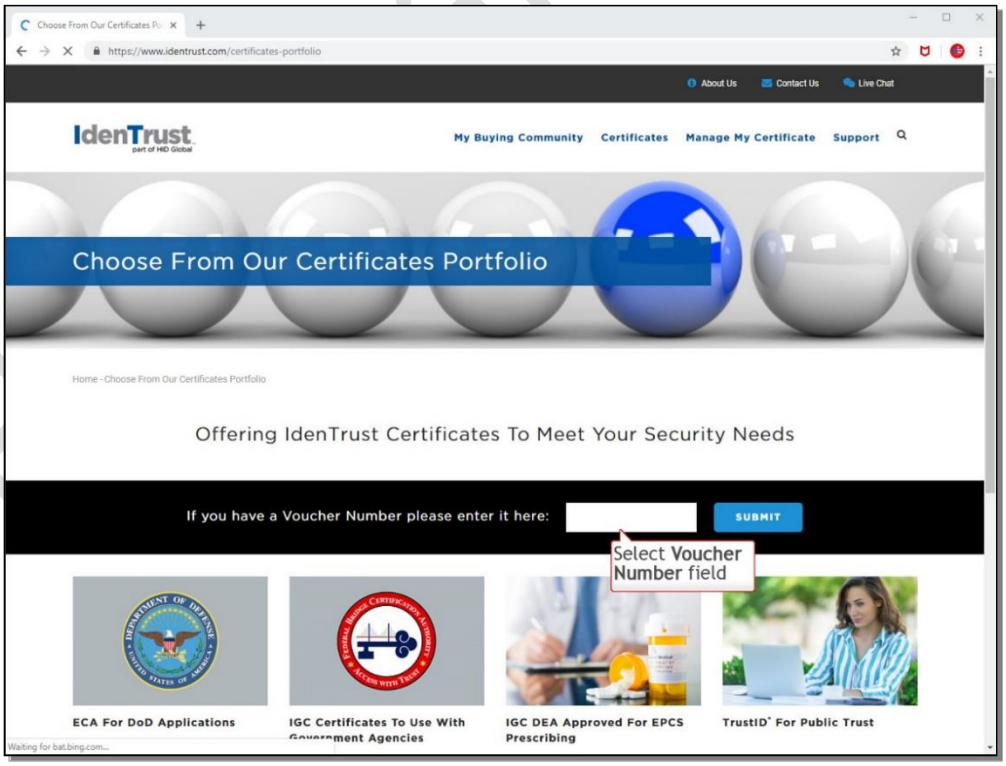
1. How to Digitally Sign Documents
2. Import and Export a Software Certificate
3. Manage My DoD ECA Certificates
4. Manage My TLS/SSL Certificates
5. Renew, Replace or Initiate a Key Recovery
6. Sign and Encrypt Email Communications
7. Policies – Current and Archived
8. DoD ECA Certificate Fact Sheet
9. DoD ECA Identity Verification Requirements
10. FAQs for ECA

FINAL Staffing Draft

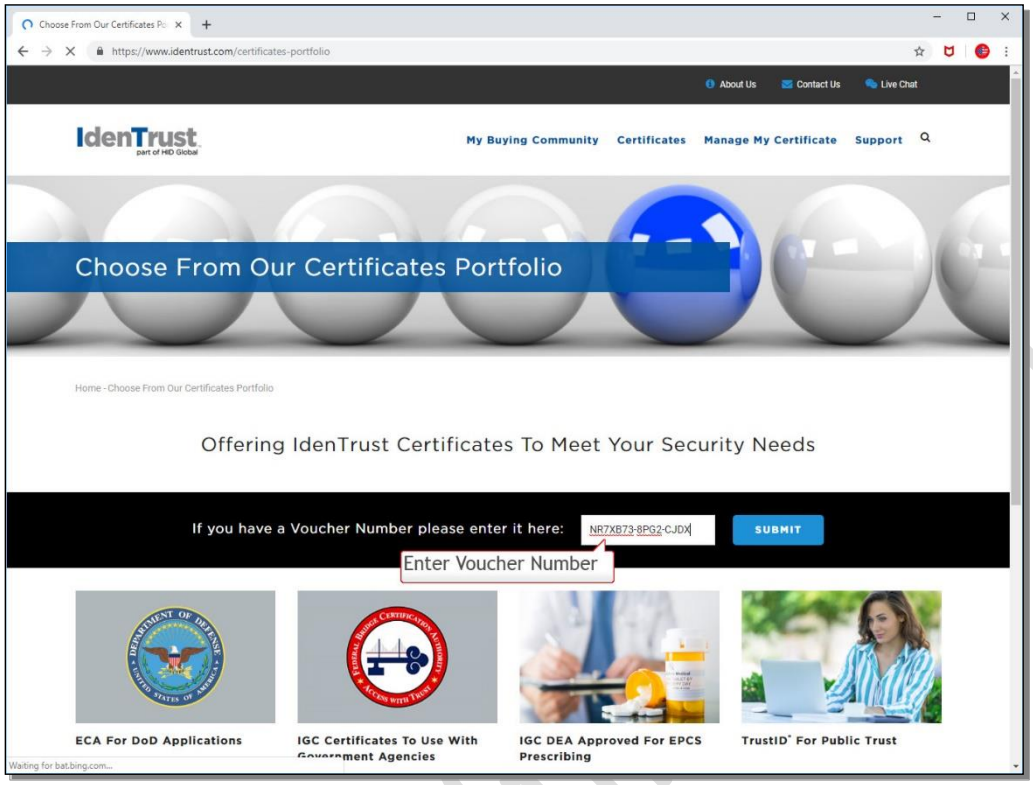
Slide1



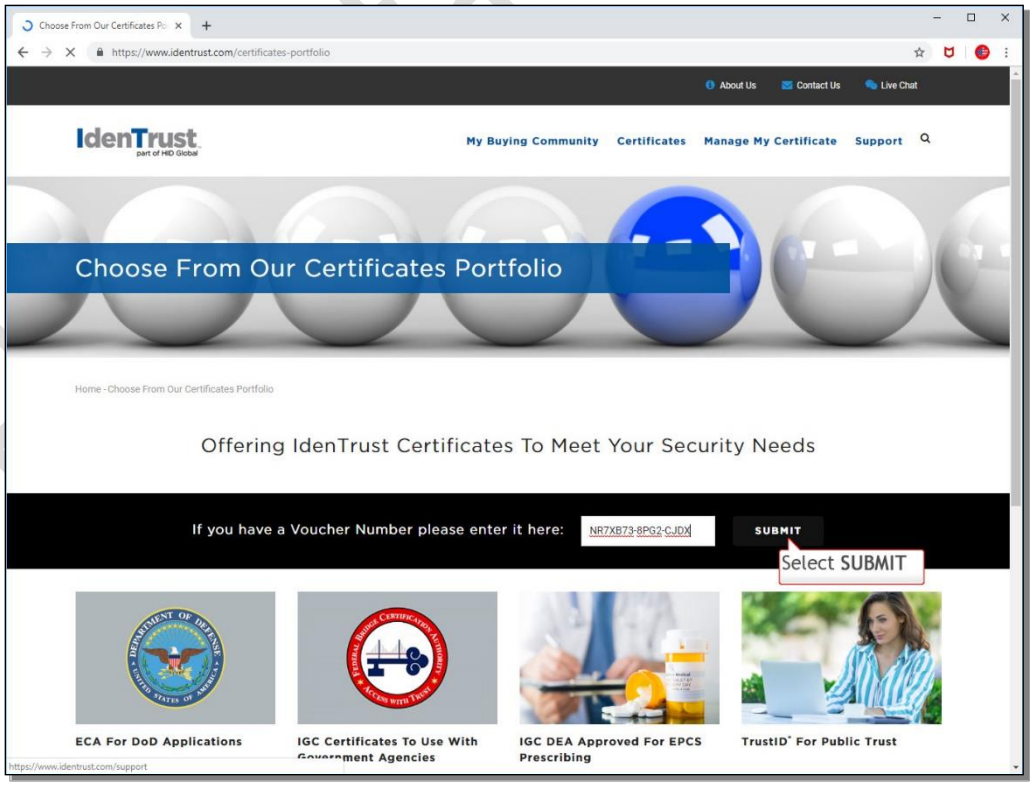
Slide2



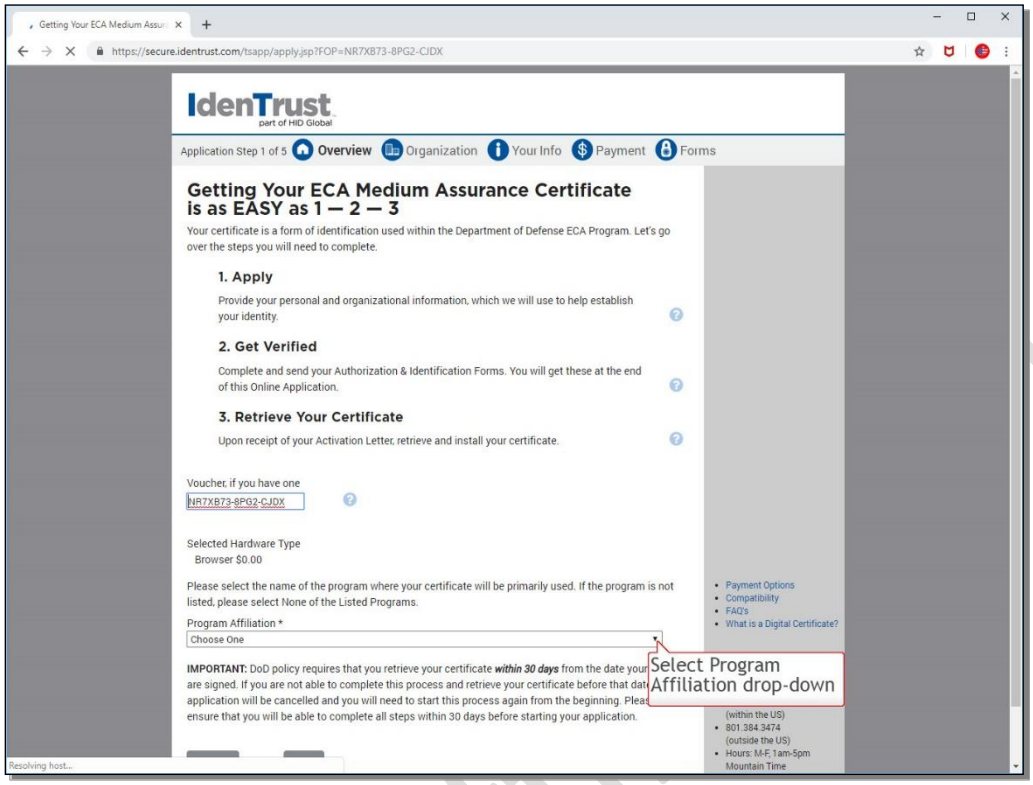
Slide3



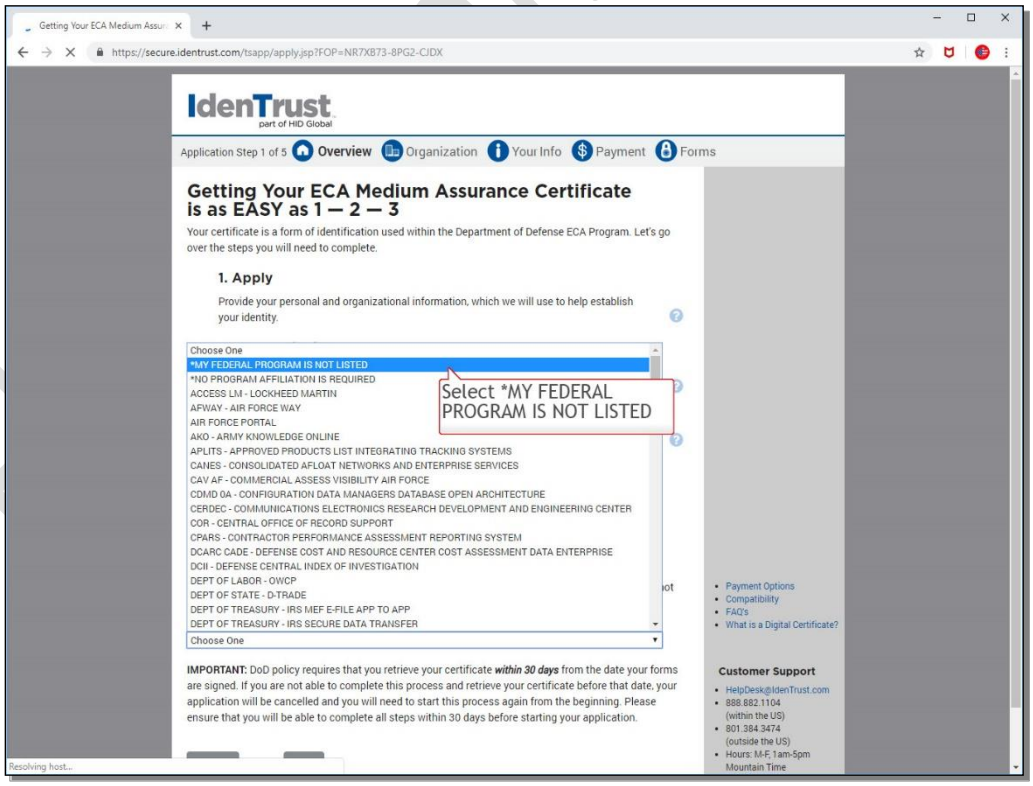
Slide4



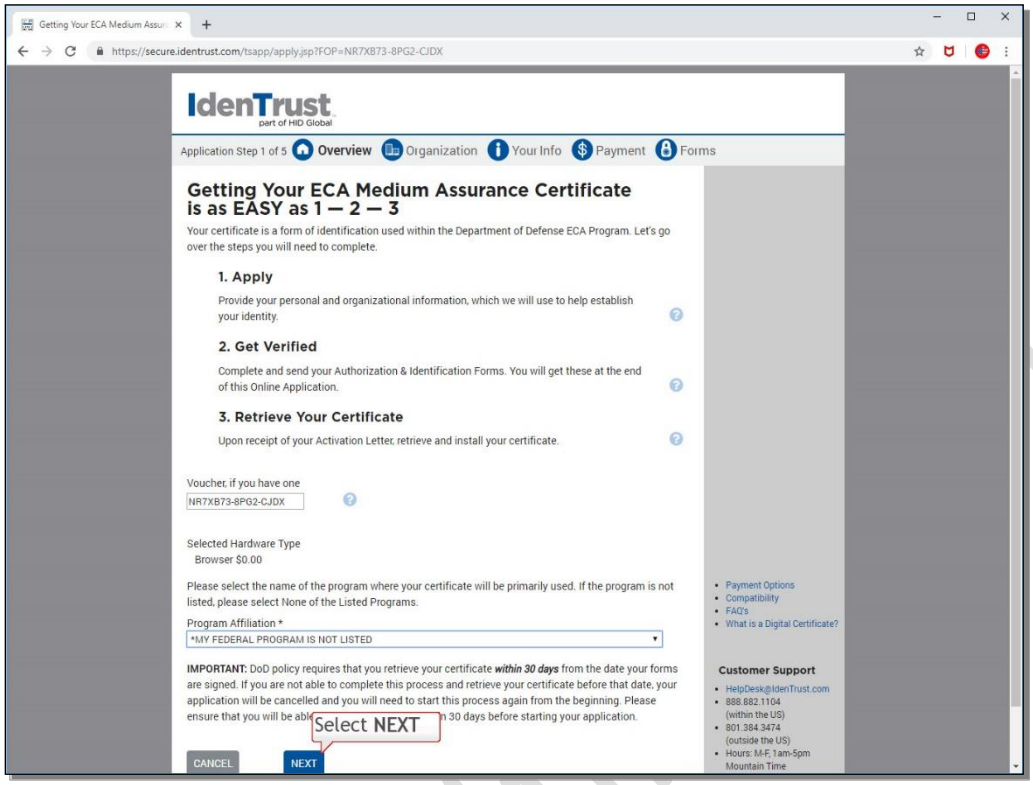
Slide5



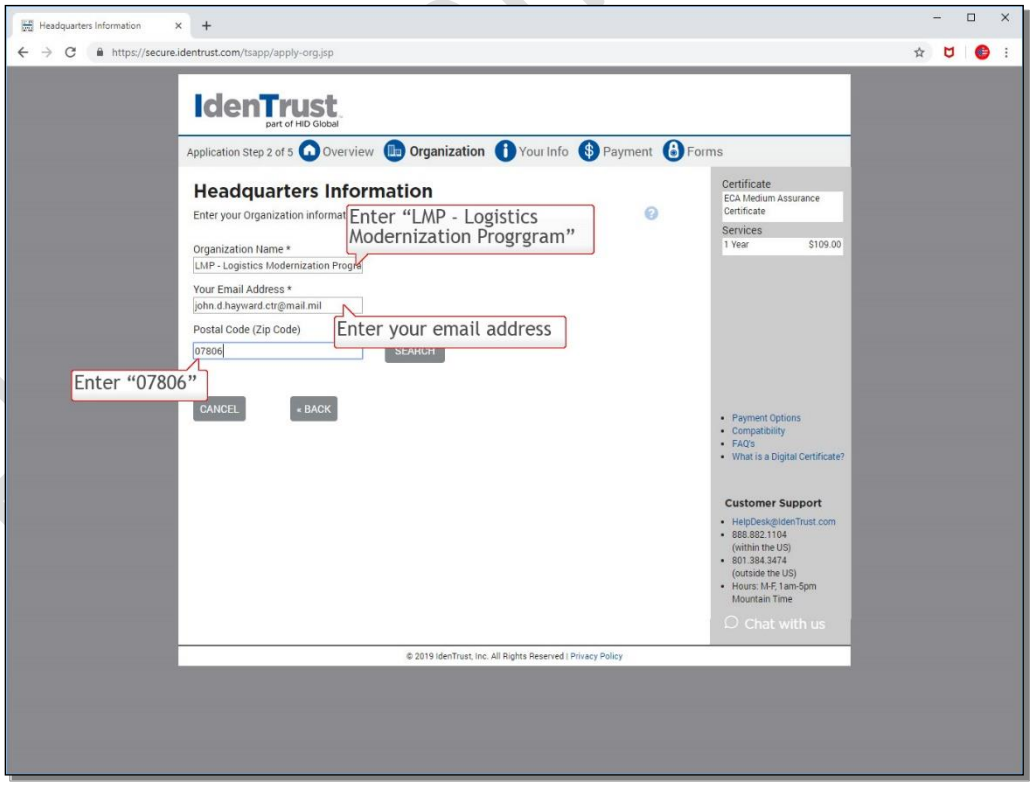
Slide6



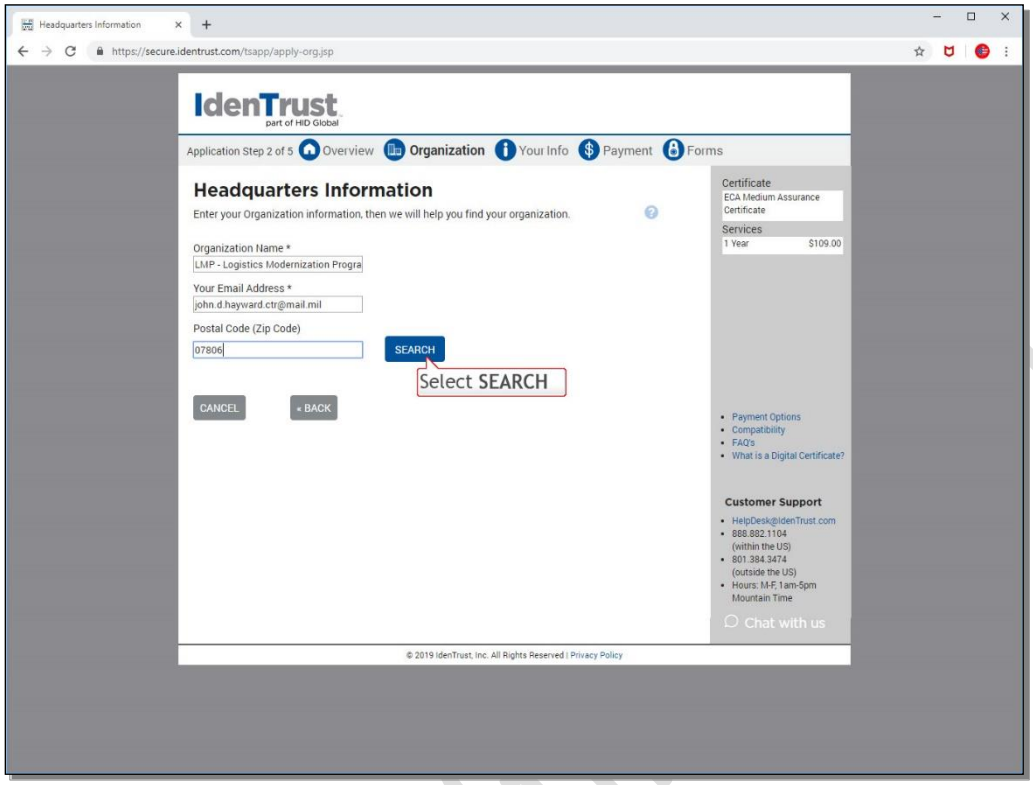
Slide7



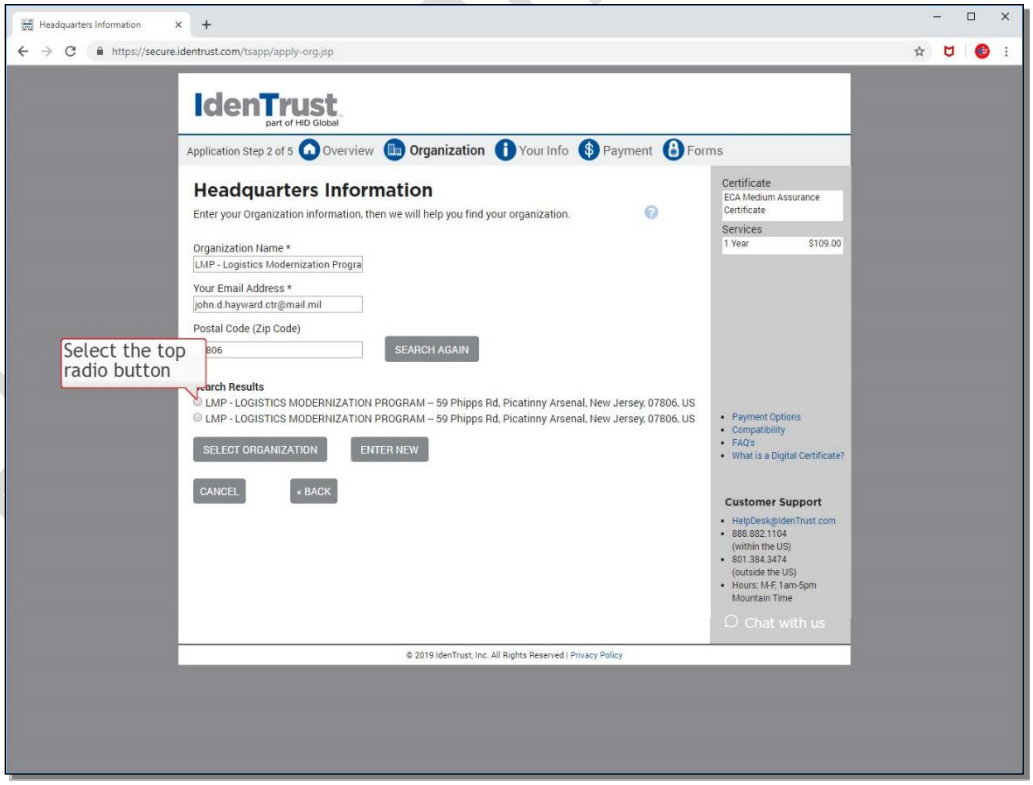
Slide8



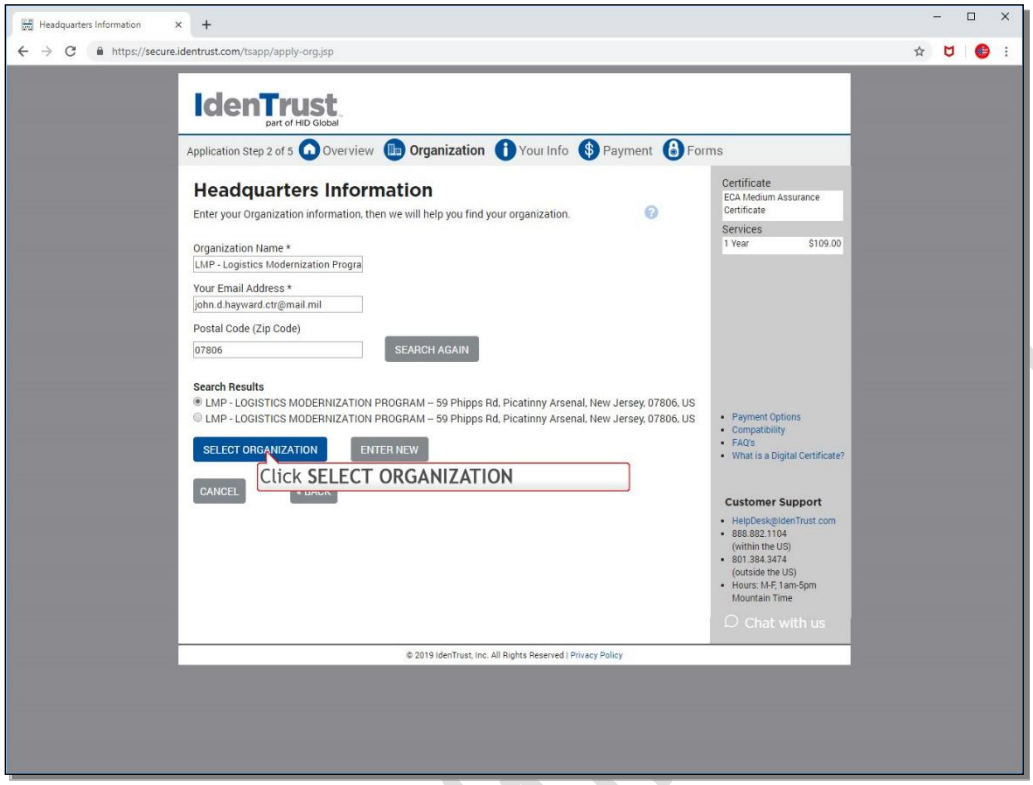
Slide9



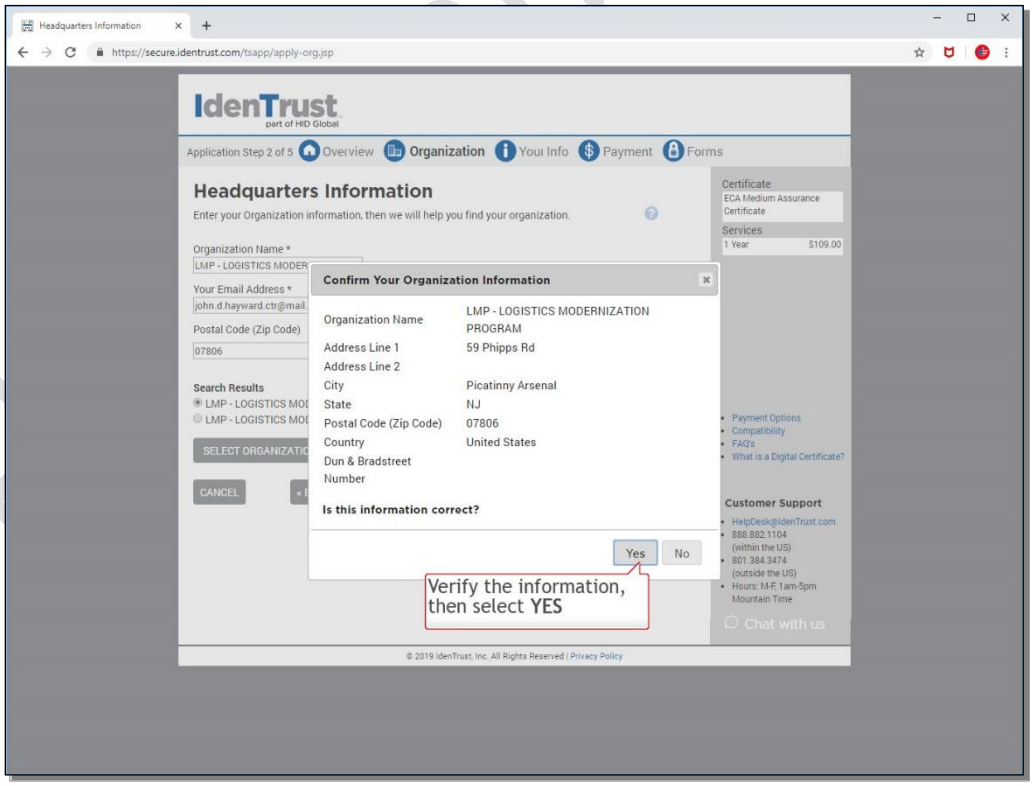
Slide10



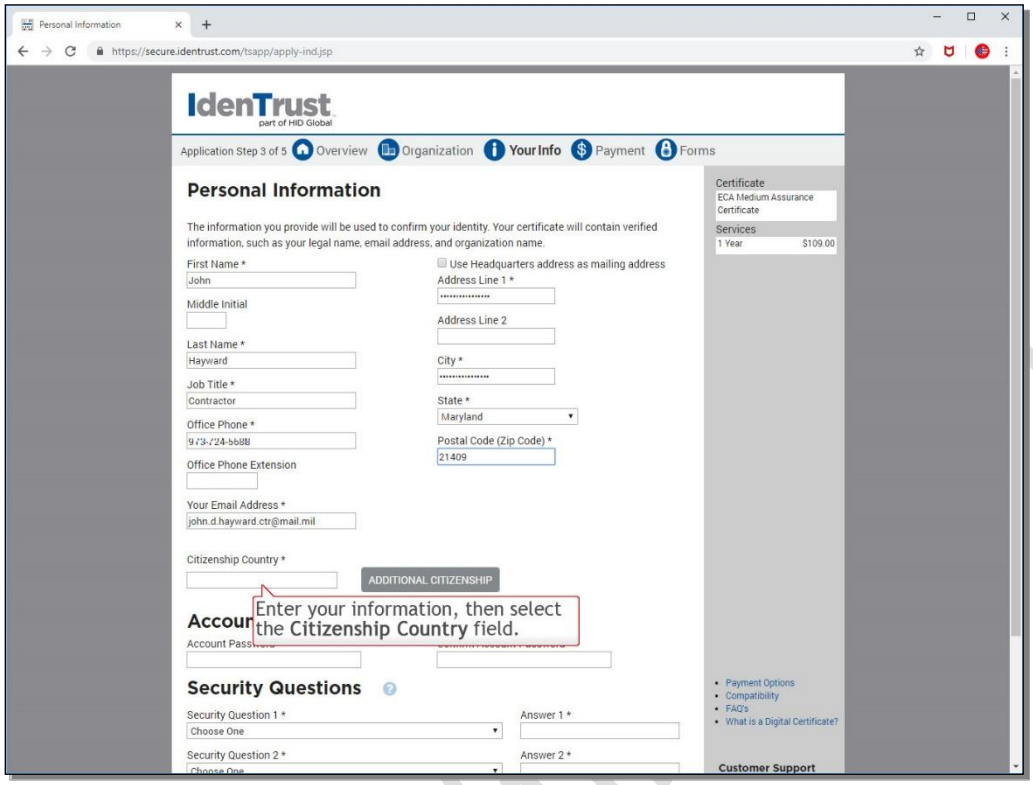
Slide11



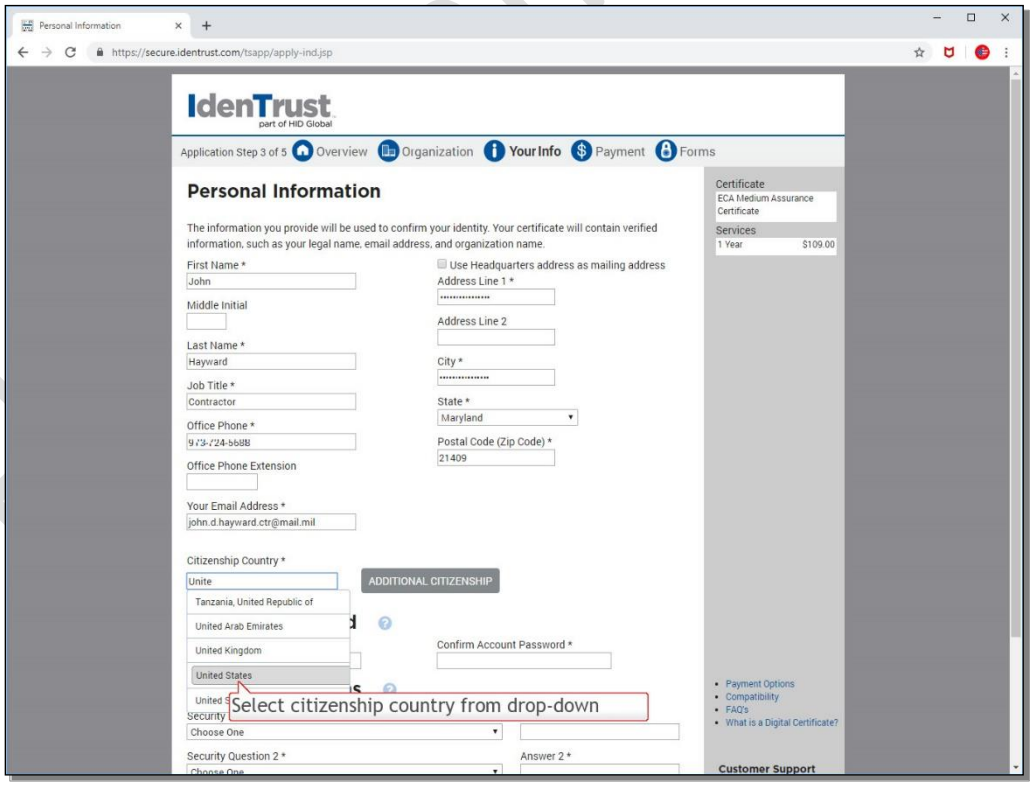
Slide12



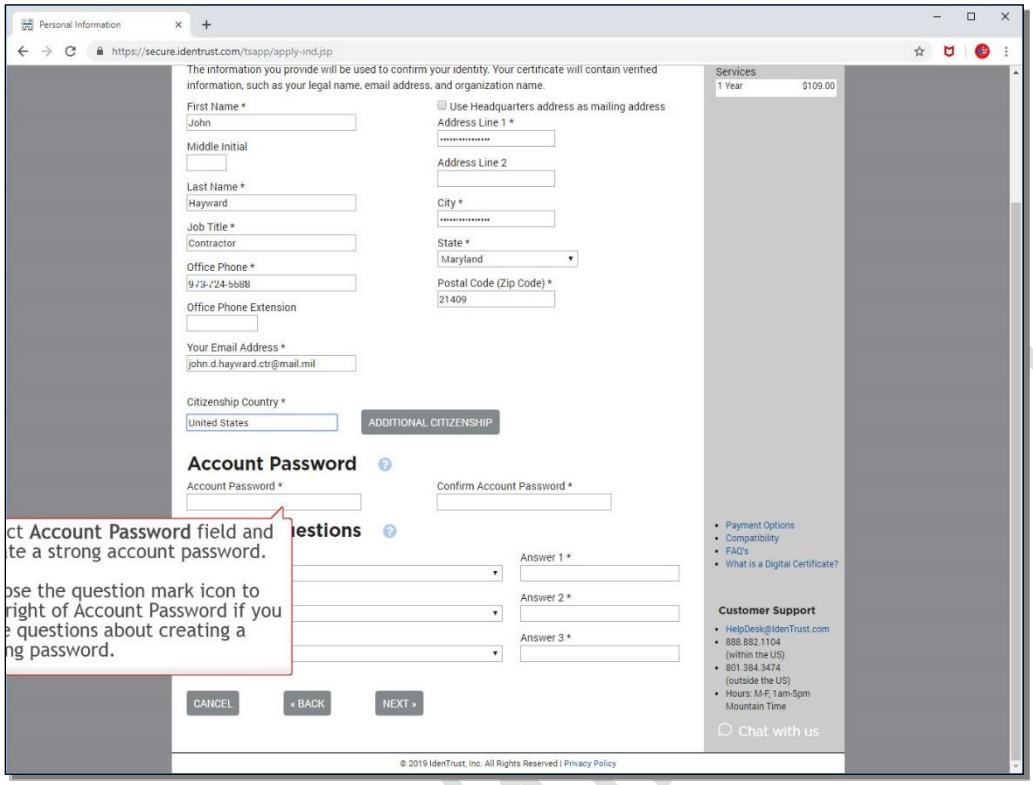
Slide13



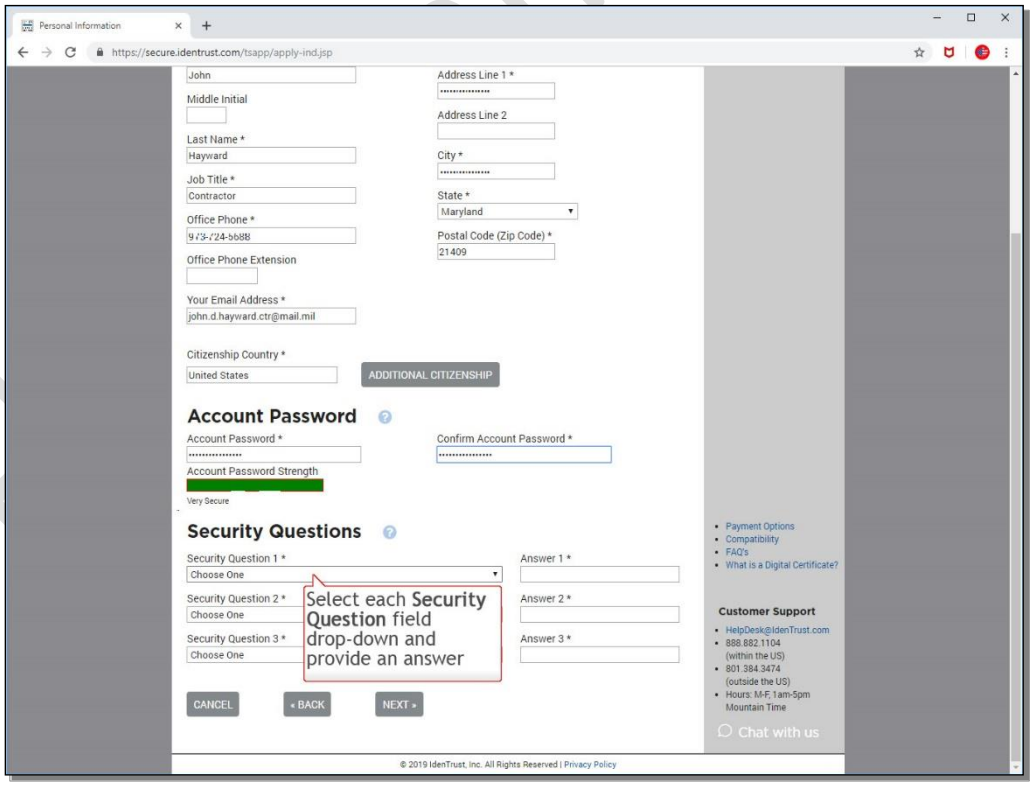
Slide14



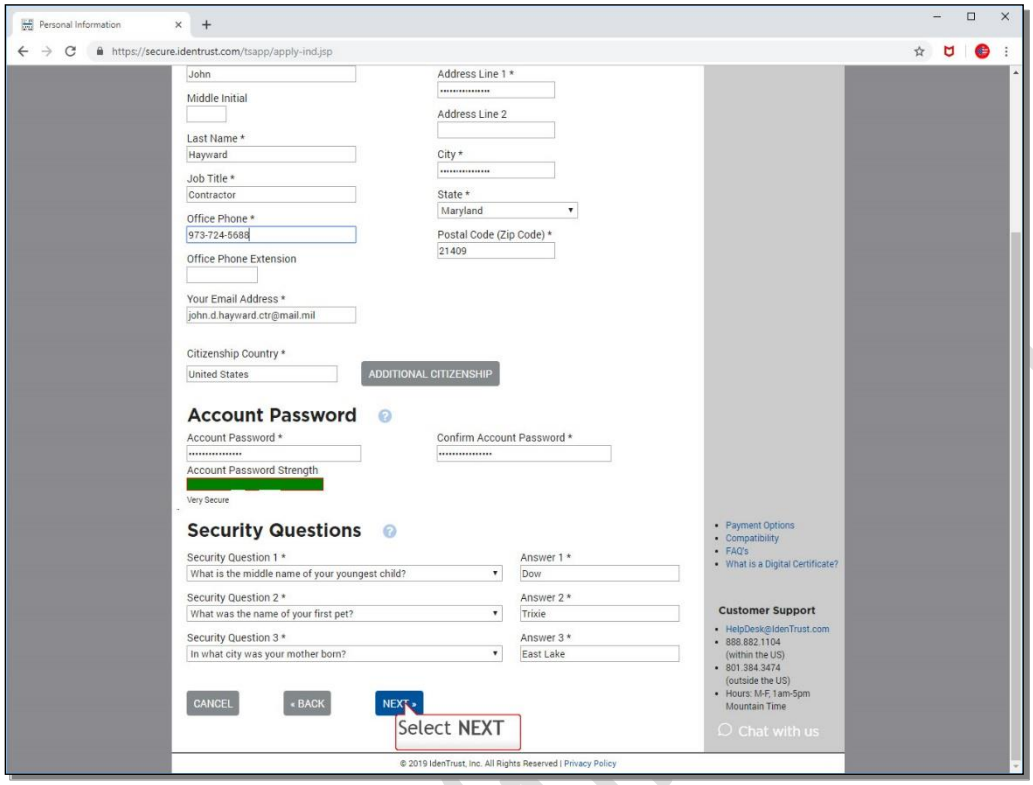
Slide15



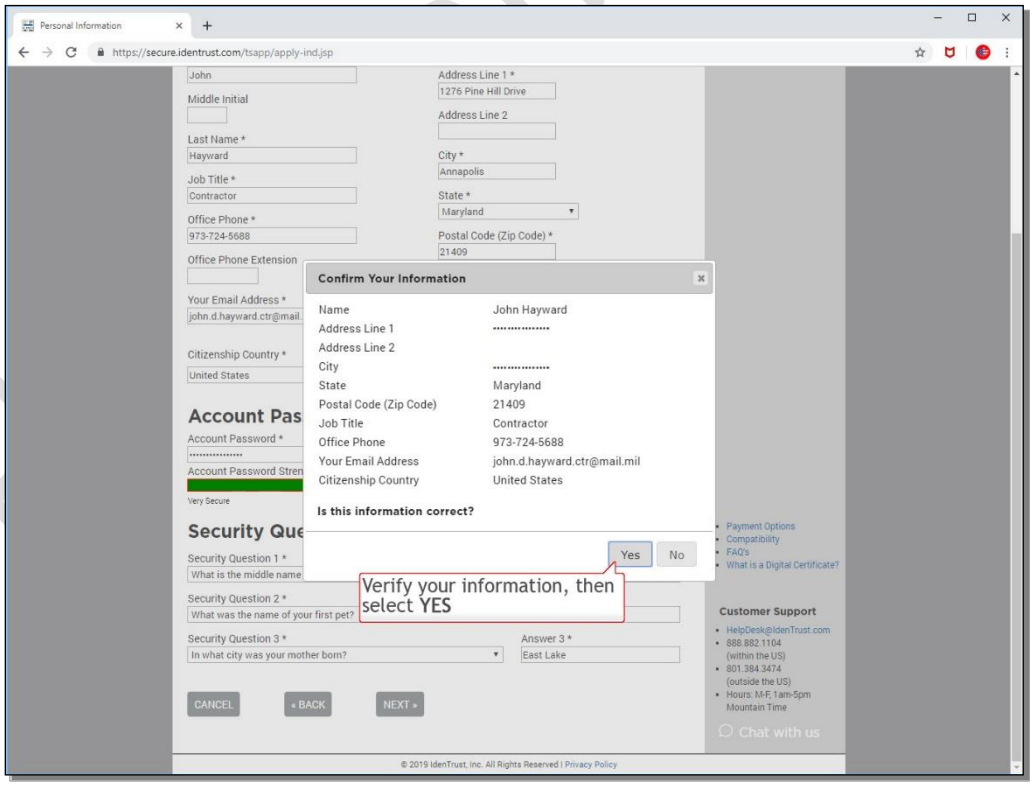
Slide16



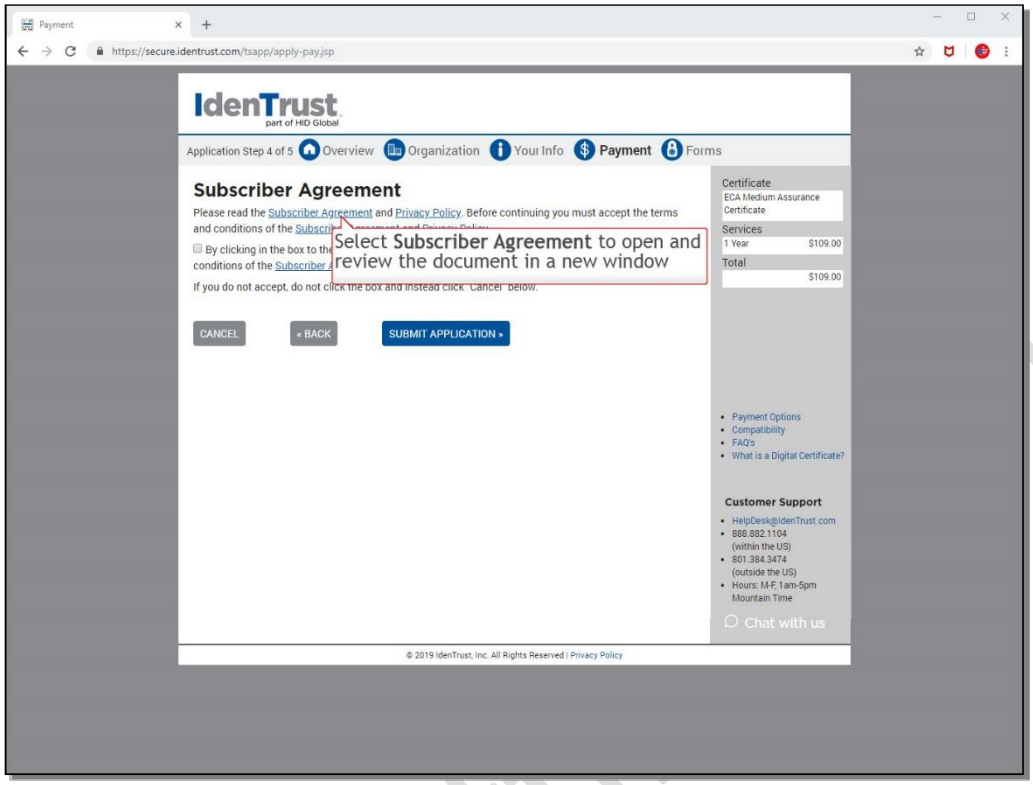
Slide17



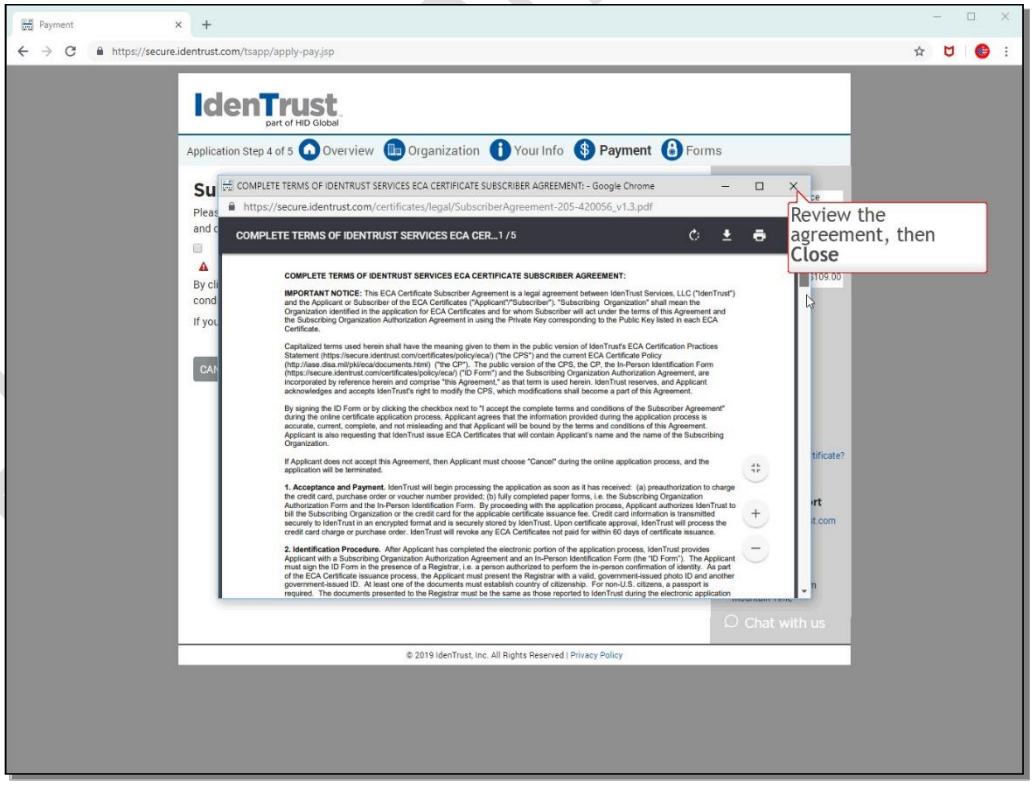
Slide18



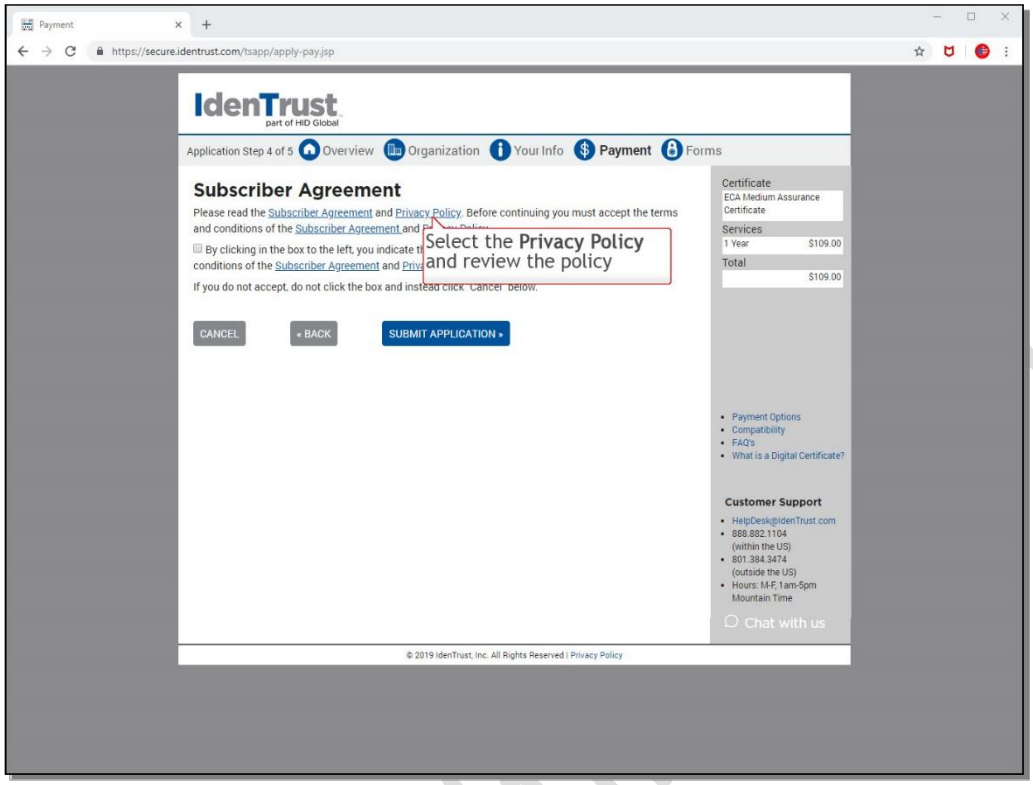
Slide19



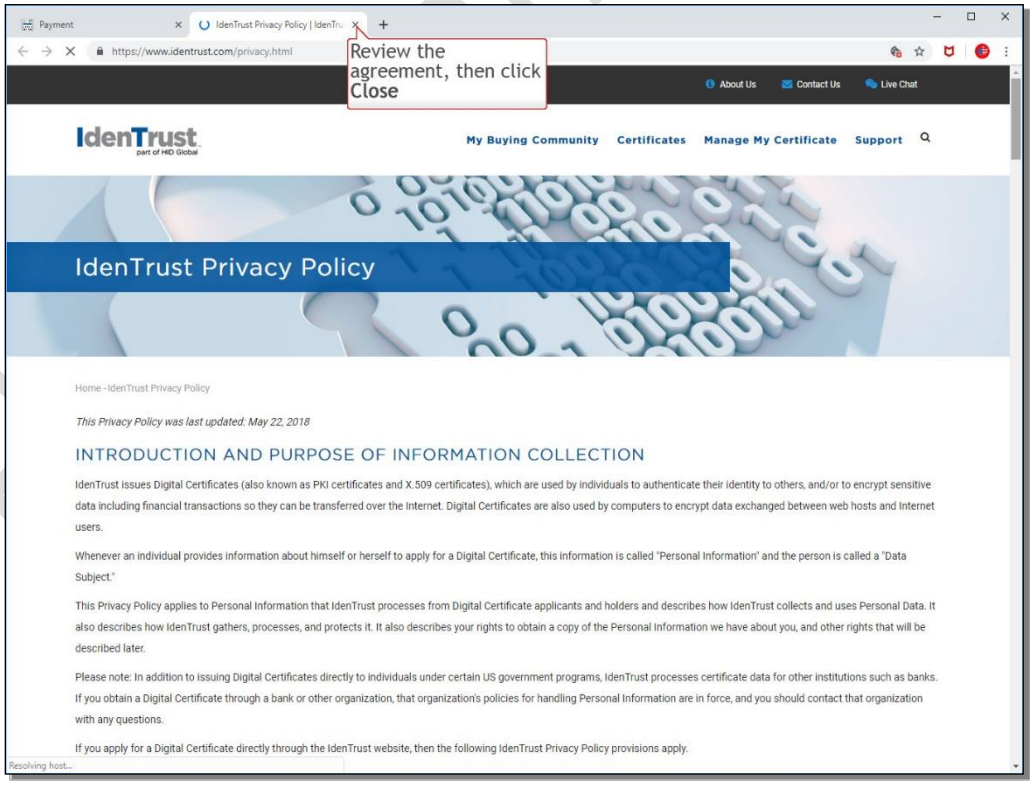
Slide20



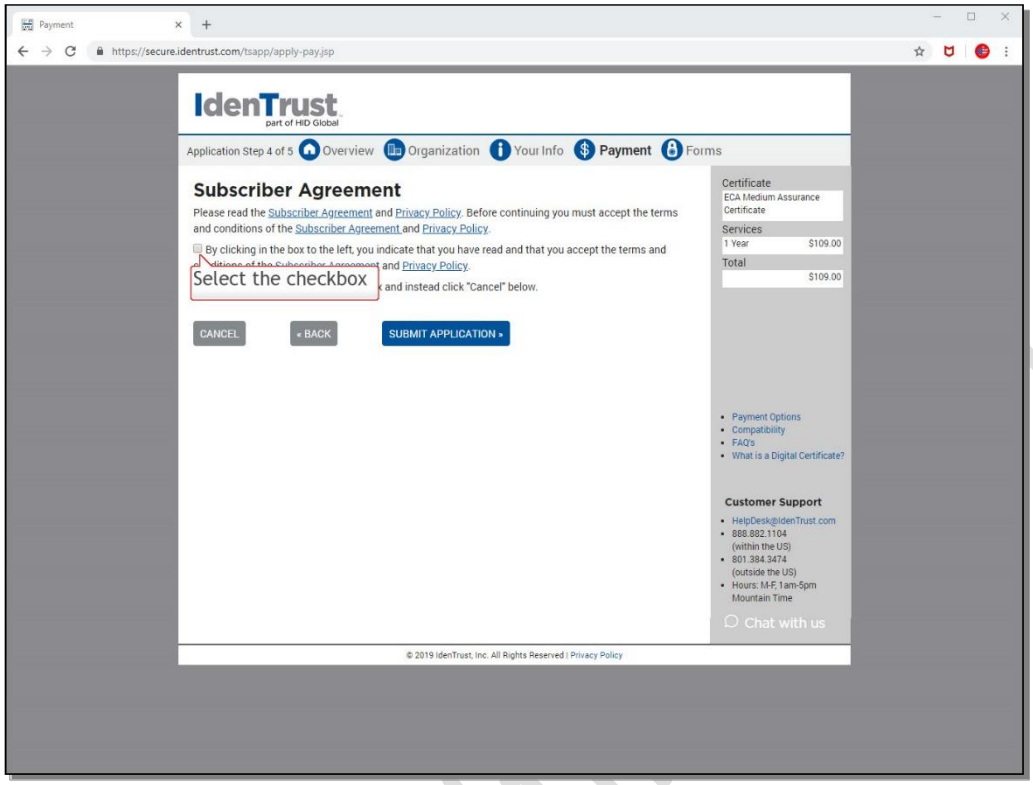
Slide21



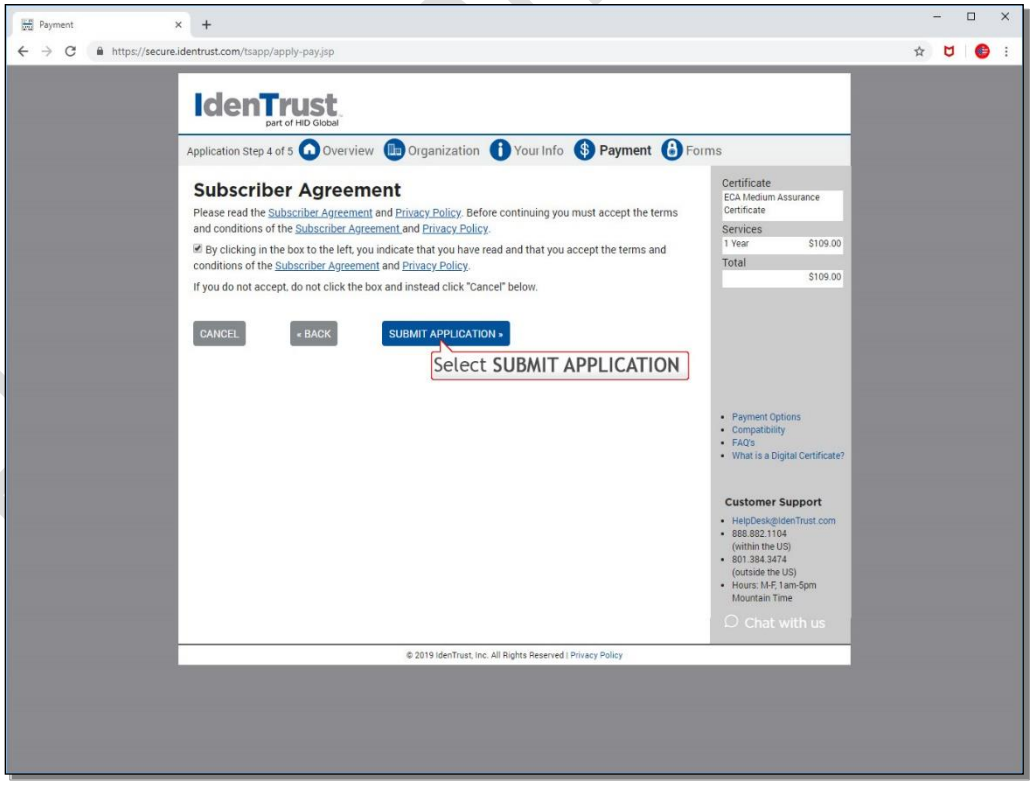
Slide22



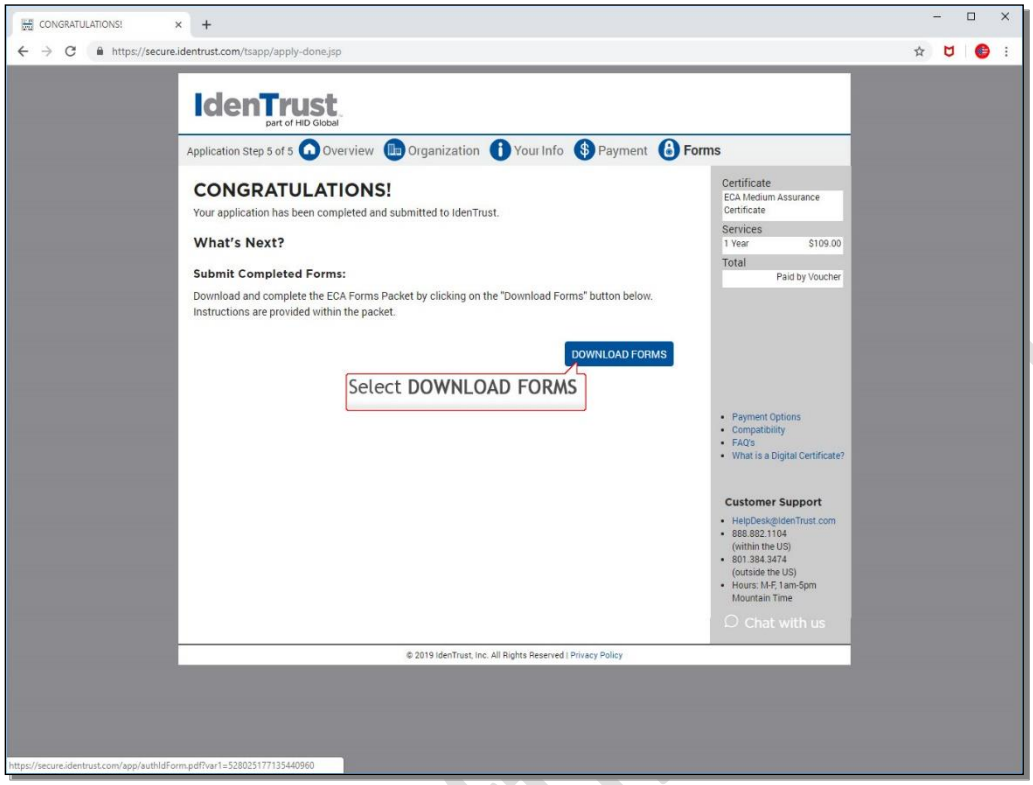
Slide23



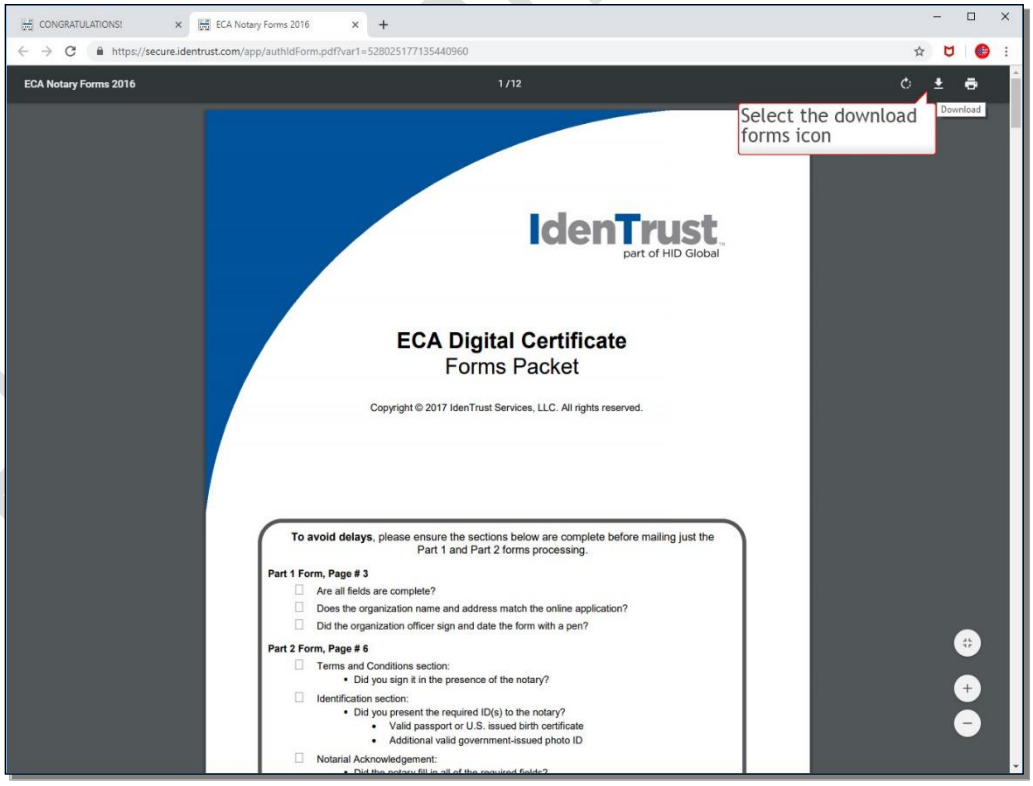
Slide24



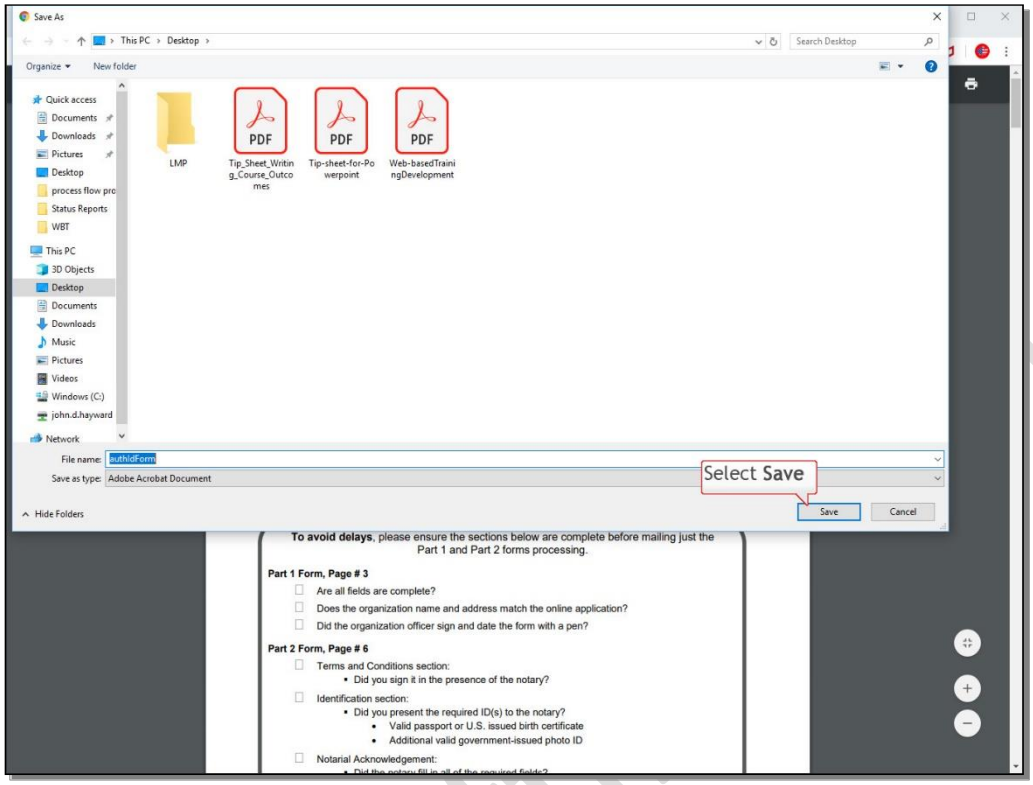
Slide25



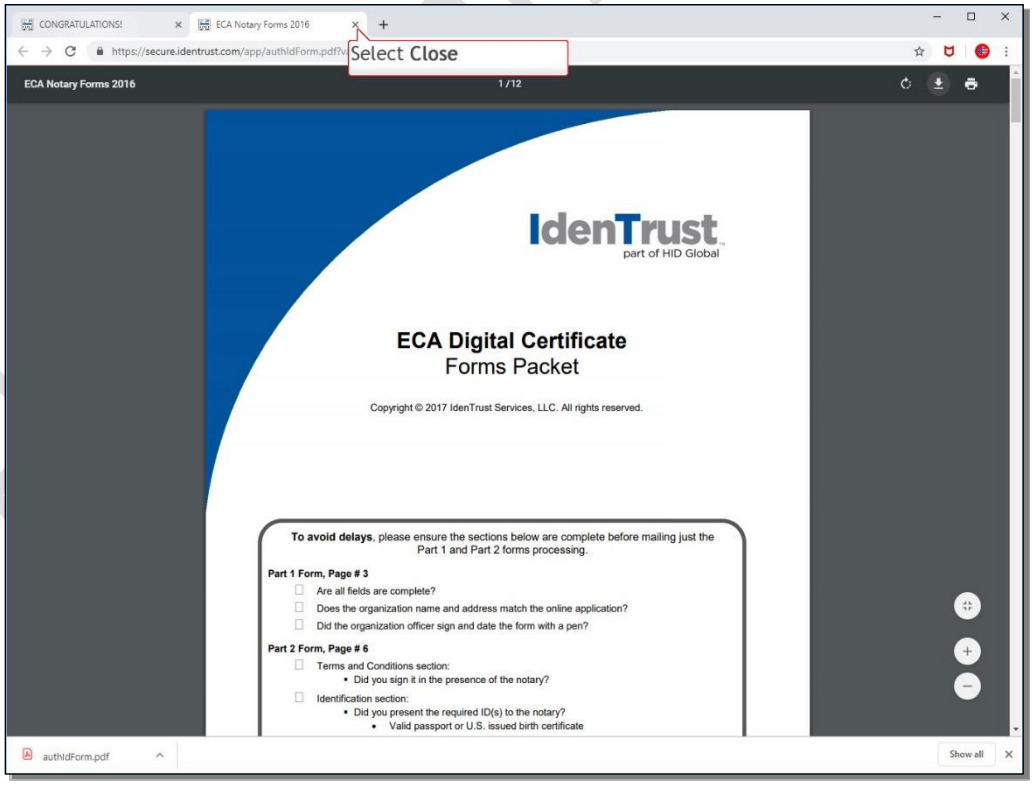
Slide26



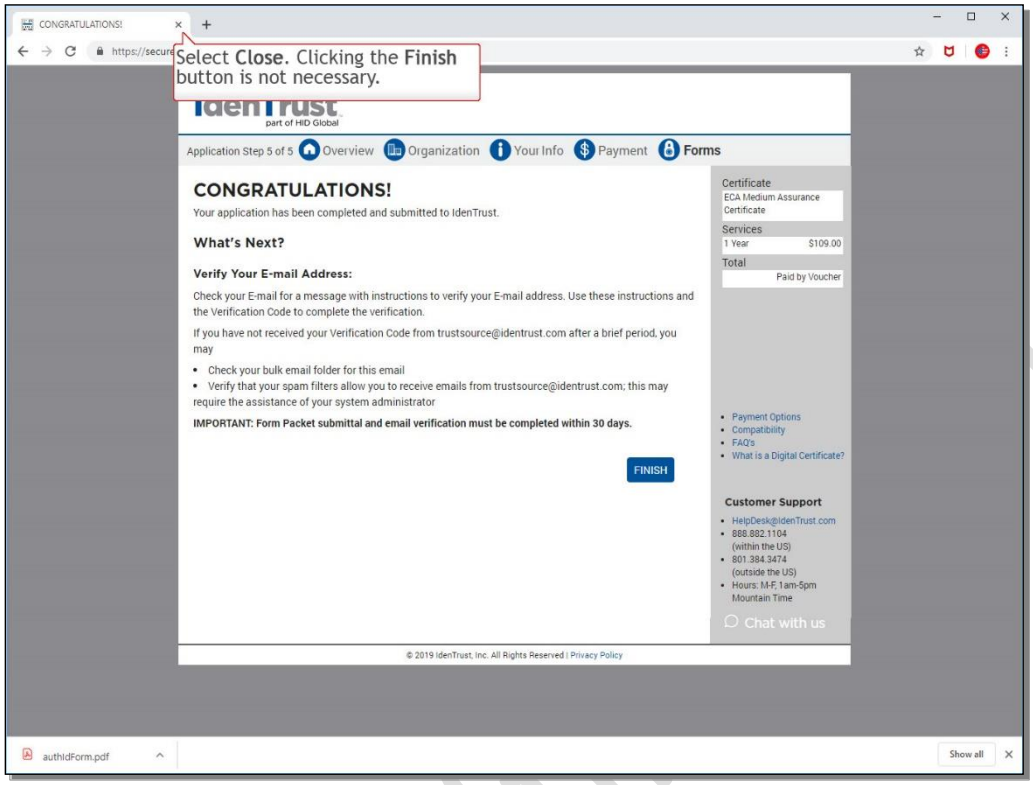
Slide27



Slide28



Slide29



FINAL Staff

Appendix B – TAV-C Portal User Role to Training Course Matrix

Training Course ID	Training Course Title	Audience	FSR UAM Tech Name(s)
LMP_TAVC_EDU_109_WBT	TAV-C Portal - SSI Contractor Overview	All Portal SSI Contractors	N/A
LMP_TAVC_IMWM_316_WBT	TAV-C Portal - Cycle Count Leader	SSI Contractors - Cycle Count Leaders	QRF-IMWM00000071
LMP_TAVC_IMWM_317_WBT	TAV-C Portal - Cycle Count Manager	SSI Contractors - Cycle Count Managers	QRF-IMWM00000070
LMP_TAVC_IMWM_319_WBT	TAV-C Portal - Receiving Specialist	SSI Contractors - Receiving Specialists	QRF-IMWM00000072
LMP_TAVC_IMWM_318_WBT	TAV-C Portal - Inventory Processor	SSI Contractors - Inventory Processors	QRF-IMWM00000069
LMP_TAVC_DIST_323_WBT	TAV-C Portal - Delivery Processor	SSI Contractors - Delivery Processors	QRF-IMWM00000063
LMP_TAVC_DIST_324_WBT	TAV-C Portal - Denial Processor	SSI Contractors - Denial Processors	QRF-IMWM00000065
LMP_TAVC_DIST_325_WBT	TAV-C Portal - Cancellation Processor	SSI Contractors - Cancellation Processors	QRF-IMWM00000066
LMP_TAVC_DIST_326_WBT	TAV-C Portal - Ship-in-Place Processor	SSI Contractors - Ship in Place Delivery Processors	QRF-IMWM00000067
LMP_TAVC_IWMW_320_WBT	TAV-C Portal - Reports	SSI Contractors - Reporting	URF-ALL-00000004
LMP_TAVC_DIST_204_WBT	TAV-C Portal - Vendor/Contractor Proof of Delivery	All Vendor/Contractors using Portal Proof of Delivery	QRF-DIST00000064 QRF-DIST00000069

FINAL Staffing Draft

Appendix C – SAMPLE DoD ECA Forms Packet

ECA-Digital-Certific
ate-Forms-Packet-20

FINAL Staffing Draft

Appendix D – Acronym List

Acronym	Name
ACC	Army Contracting Command
AMC	Army Materiel Command
CA	Cyber Awareness
CAC	Common access card
COR	Contracting Officer's Representative
DoD	Department of Defense
ECA	External Certification Authority
FSR	Functional Security Roles
HQ	Headquarters
IA	Information Assurance
SAAR	System Authorization Access Request
TAV-C	Total Asset Visibility – Contractor
UAM	User Account Manager

FINAL