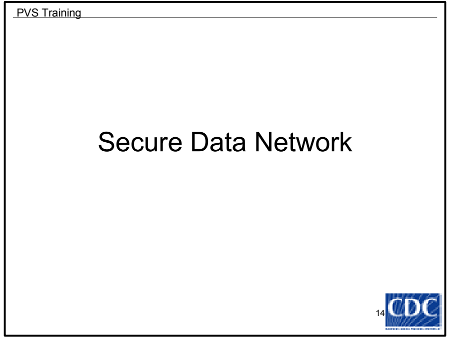
PRE-EVENT VACCINATION SYSTEM TRAINING FOR LOCAL ADMINISTRATORS

PART 3

Slide 14

V. Secure Data Network (SDN)

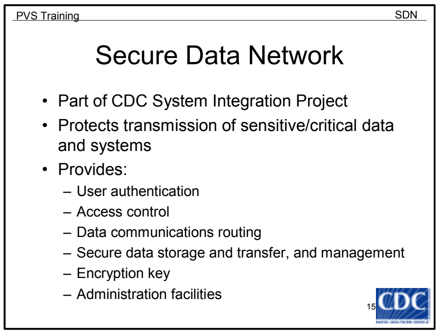


PVS Training

Secure Data Network

14

Slide 15



PVS Training SDN

Secure Data Network

- Part of CDC System Integration Project
- Protects transmission of sensitive/critical data and systems
- Provides:
  - User authentication
  - Access control
  - Data communications routing
  - Secure data storage and transfer, and management
  - Encryption key
  - Administration facilities

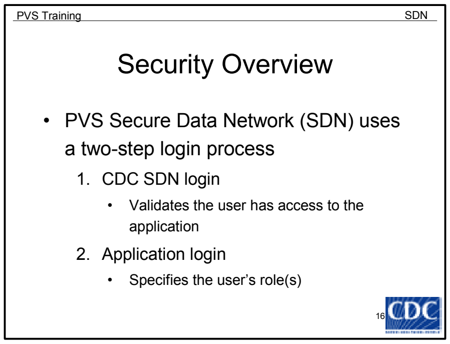
15

A. Part of the CDC Surveillance System Integration Project

B. A secure Internet connection and gateway facility which protects transmissions of sensitive or critical data and sensitive or critical systems

C. The SDN provides:
   1. User authentication
   2. Access control (authorization)
   3. Data communications routing
   4. Secure data storage and transfer and management of sensitive data
   5. Encryption key management
   6. Administration facilities

Slide 16



PVS Training SDN

Security Overview

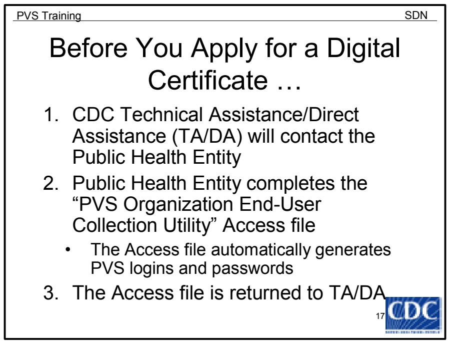
- PVS Secure Data Network (SDN) uses a two-step login process
  1. CDC SDN login
     - Validates the user has access to the application
  2. Application login
     - Specifies the user's role(s)

16

D. Security Overview
   1. The PVS Secure Data Network uses a two-step login process
      a) CDC Secure Data Network (SDN) Login
      b) Application Login
   2. Step 1: The user installs a digital certificate on their machine. The digital certificate is used to access the PVS application.
      a) Digital Certificates are managed and distributed by the SDN group at CDC and are specific to one user on a specific machine
         1) Digital certificates validate the user's identity, ensuring the data sent is from a legitimate source.
      b) When the user initiates the PVS URL, they are prompted for the password (challenge phrase) that corresponds to the digital certificate.
      c) The authentication process validates that the user has access to the application. Once validated, the user is given access to the PVS application.
      d) The PVS application prompts the user for a second level of authentication.

3. Step 2: The user enters an application username and password
   a) This second level of authentication determines the roles that have been assigned to the user.
   b) The roles dictate what the user can do and what data the user can view within the system.
   c) The CDC PVS Administrator manages application level logins.

Slide 17



PVS Training SDN

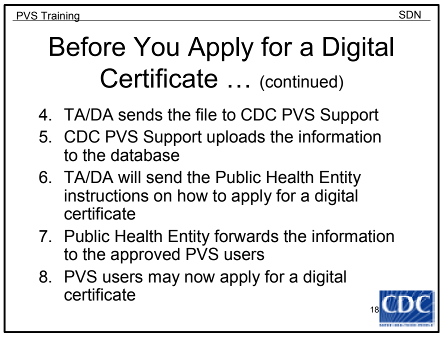
Before You Apply for a Digital Certificate …

1. CDC Technical Assistance/Direct Assistance (TA/DA) will contact the Public Health Entity
2. Public Health Entity completes the "PVS Organization End-User Collection Utility" Access file
   - The Access file automatically generates PVS logins and passwords
3. The Access file is returned to TA/DA

17

E. Before you apply for a digital certificate...
   1. CDC Technical Assistance/Direct Assistance (TA/DA) will contact the Public Health Entity and ask them to complete the "PVS Organization End User Collection Utility" Access file
      a) The Access utility captures information such as PVS user's name, user role, and generates the user's PVS login and password.
      b) The PVS password may not be changed.
      c) The Public Health Organization is entered in the access utility.
      d) All affiliated organizations are entered in the access application. These include:
         1) Organizations that refer employees to be vaccinated
         2) Organizations that are vaccination clinics
         3) Organizations that will be responsible for interpreting the take response to the vaccination
   2. Public Health Entity completes the "PVS Organization End-User Collection Utility" Access file
   3. The Access utility is returned to TA/DA

Slide 18



PVS Training SDN

Before You Apply for a Digital Certificate … (continued)

4. TA/DA sends the file to CDC PVS Support
5. CDC PVS Support uploads the information to the database
6. TA/DA will send the Public Health Entity instructions on how to apply for a digital certificate
7. Public Health Entity forwards the information to the approved PVS users
8. PVS users may now apply for a digital certificate

18

4. TA/DA sends the file to CDC PVS Support
5. After the information has been approved, CDC PVS Support uploads the information to the database
6. TA/DA sends the Public Health Entity instructions on how to apply for a digital certificate.
7. Public Health Entity forwards the information to the approved PVS users
8. PVS users may now apply for a digital certificate or add digital certificate activities
9. If the PVS user forgets their password, they will need to contact their public health entity or the CDC PVS help desk. The CDC PVS help desk will e-mail the password to the user.

VI. Applying for a Digital Certificate

Slide 19

PVS Training

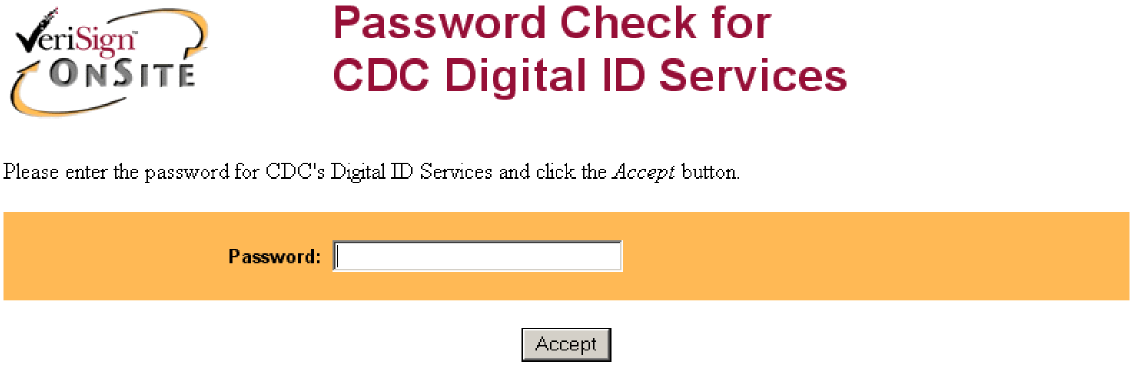
Applying for a Digital Certificate

19

A. Setting up access to the system
   1. If you already have a digital certificate for another system, such as NEDSS or EpiX, go to https://sdn.cdc.gov/ in order to request PVS activity.
   2. If should be noted that only data entry staff need digital certificates.
      a) Vaccinators and take response readers do not require a digital certificate, unless they also enter data.
      b) A digital certificate must be obtained by each person who will be accessing PVS.
      c) One computer may have multiple digital certificates (DC) and a person's DC may be installed on multiple computers using the export/import function (not discussed in these materials).

Slide 20

   3. Access the SDN enrollment website at https://ca.cdc.gov/ to begin the enrollment process.
      a) You must access the SDN enrollment website and complete the enrollment process from the same computer and browser you will be using to access SDN.
   4. Enter the general registration password provided by your program administrator and click the ACCEPT button.



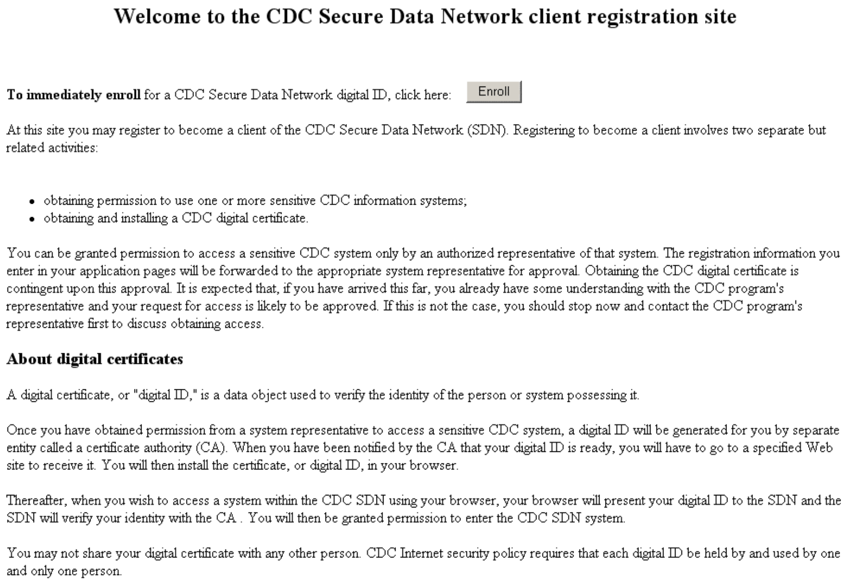
Password Check for CDC Digital ID Services

Please enter the password for CDC's Digital ID Services and click the *Accept* button.

Password:

Slide 21

5. After authentication, you will be presented with a general information page providing an overview of digital certificates and system requirements. After reviewing the enrollment information, proceed to the first enrollment step by clicking the ENROLL button.



Welcome to the CDC Secure Data Network client registration site

To immediately enroll for a CDC Secure Data Network digital ID, click here: Enroll

At this site you may register to become a client of the CDC Secure Data Network (SDN). Registering to become a client involves two separate but related activities:

- obtaining permission to use one or more sensitive CDC information systems;
- obtaining and installing a CDC digital certificate.

You can be granted permission to access a sensitive CDC system only by an authorized representative of that system. The registration information you enter in your application pages will be forwarded to the appropriate system representative for approval. Obtaining the CDC digital certificate is contingent upon this approval. It is expected that, if you have arrived this far, you already have some understanding with the CDC program's representative and your request for access is likely to be approved. If this is not the case, you should stop now and contact the CDC program's representative first to discuss obtaining access.

About digital certificates

A digital certificate, or "digital ID," is a data object used to verify the identity of the person or system possessing it.

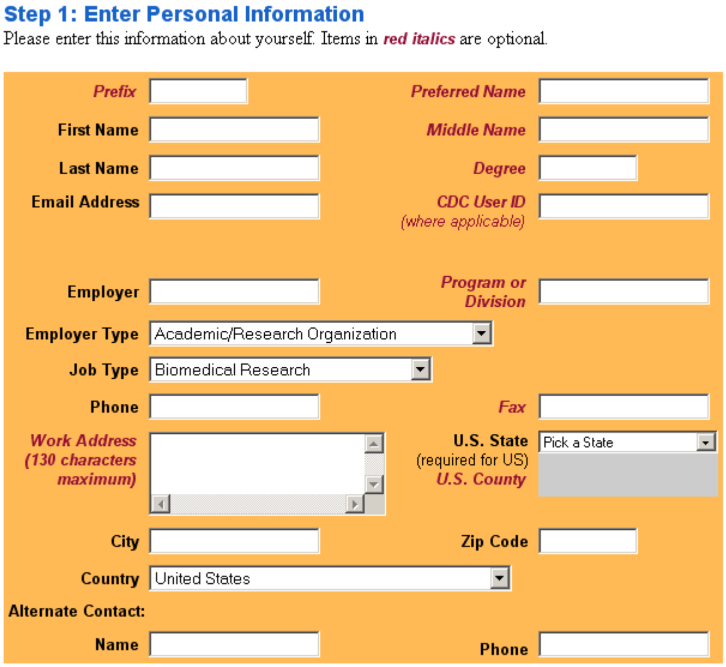
Once you have obtained permission from a system representative to access a sensitive CDC system, a digital ID will be generated for you by separate entity called a certificate authority (CA). When you have been notified by the CA that your digital ID is ready, you will have to go to a specified Web site to receive it. You will then install the certificate, or digital ID, in your browser.

Thereafter, when you wish to access a system within the CDC SDN using your browser, your browser will present your digital ID to the SDN and the SDN will verify your identity with the CA . You will then be granted permission to enter the CDC SDN system.

You may not share your digital certificate with any other person. CDC Internet security policy requires that each digital ID be held by and used by one and only one person.

Slide 22

6. <u>Step 1- Enter Personal Information</u>: Next you must complete the "Personal Information" form to continue the enrollment process. The form is used to create your digital certificate and should be completed with as much information as possible (all optional information is identified by *red italics*). This information will be used by your program administrator and CDC to verify your identity.
   a) It should be noted that you must enter a valid e-mail address in order to apply for a digital certificate.



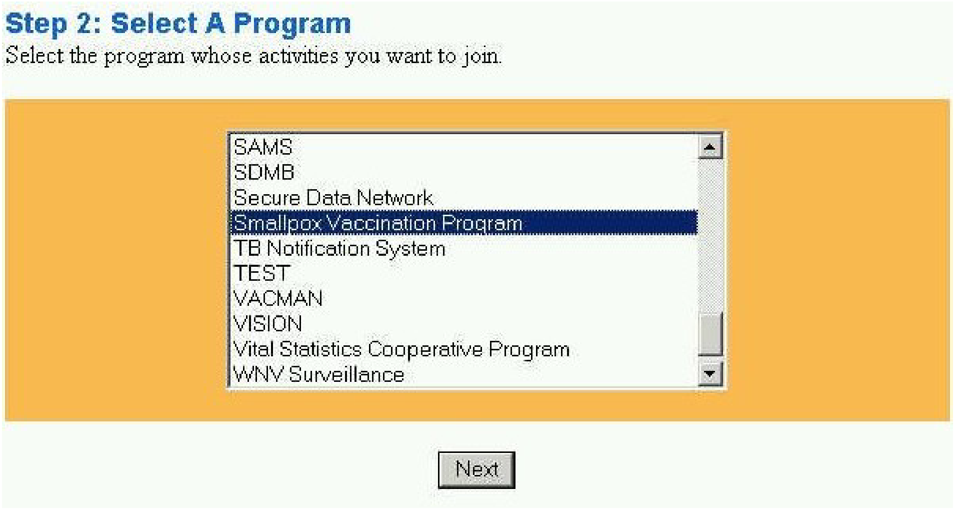
Step 1: Enter Personal Information

Please enter this information about yourself. Items in ***red italics*** are optional.

Prefix		*Preferred Name*	
First Name		*Middle Name*	
Last Name		*Degree*	
Email Address		*CDC User ID* *(where applicable)*	
Employer		*Program or Division*	
Employer Type	Academic/Research Organization		
Job Type	Biomedical Research		
Phone		*Fax*	
Work Address (130 characters maximum)		U.S. State (required for US) *U.S. County*	Pick a State
City		Zip Code	
Country	United States		
Alternate Contact:			
Name		Phone	

Slide 23

7. Step 2 - Select a Program: The list box below the personal information form allows you to choose the program for which you are requesting access. To select the program, simply highlight the appropriate entry in the list box. For the PVS System, select Smallpox Vaccination Program.
   a) Upon initial enrollment, you may only select one program from the available list. If you require access to more than one program, select the program identified by your program administrator. After obtaining your digital certificate, you will be able to request additional programs and activities via SDN (it is not necessary to apply for more than one digital certificate).
8. After completing the personal information form and selecting the program to which you are applying (e.g., Smallpox Vaccination Program), click the NEXT button to continue. A confirmation dialog will appear to verify the Email address provided on the personal information form is valid.

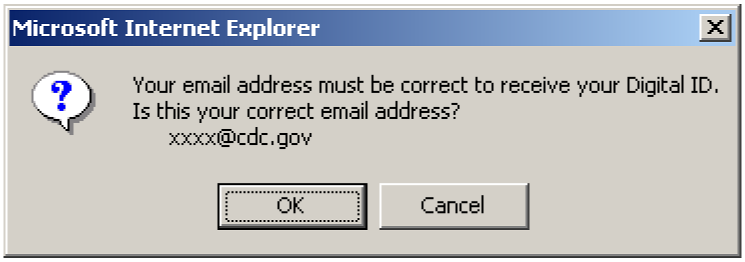


Step 2: Select A Program

Select the program whose activities you want to join.

Slide 24

9. It is important that the e-mail address you provide is accurate and used in conjunction with the performance of you duties.
10. Upon confirmation of your Email address, click the OK button to continue.



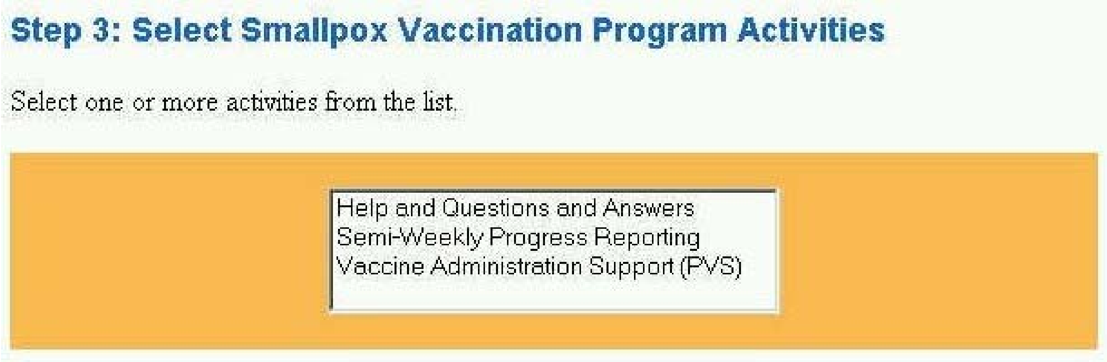
Microsoft Internet Explorer

Your email address must be correct to receive your Digital ID.
Is this your correct email address?
xxxx@cdc.gov

Slide 25

11. Step 3 - Select PVS Activities: To identify the program-specific activities to which you desire access, select one or more entries from the list. To select more than one activity, hold down the CNTL key while clicking the appropriate activities. You may be granted other activities based on your role within the organization. These roles will appear on your SDN login. The available activities for the PVS program include:

a) Help and Questions and Answers
   1) Provides information about the help line and frequently asked questions and answers.
   2) All PVS users will have access to this activity.
b) Semi-Weekly Progress Reporting
   1) Provides support for the electronic submission of smallpox vaccination evaluation data.
   2) These data are required semi-weekly (on Mondays and Thursdays) from each grantee.
   3) Users include:
      i) Public Health Entities (grantees)
      ii) Smallpox point of contact
      iii) Adverse events coordinators
c) Vaccine Administration Support (PVS)
   1) Provides support for the recording and management of vaccine administration data.
   2) Functionality currently provided includes
      i) Clinic/organization tracking
      ii) Vaccine/diluent lot batch management
      iii) Patient history and current vaccination tracking
      iv) Take response recording and tracking
   3) Users include:
      i) Public Health Entities (grantees)
      ii) Smallpox point of contact
      iii) PVS administrators
      iv) PVS viewers



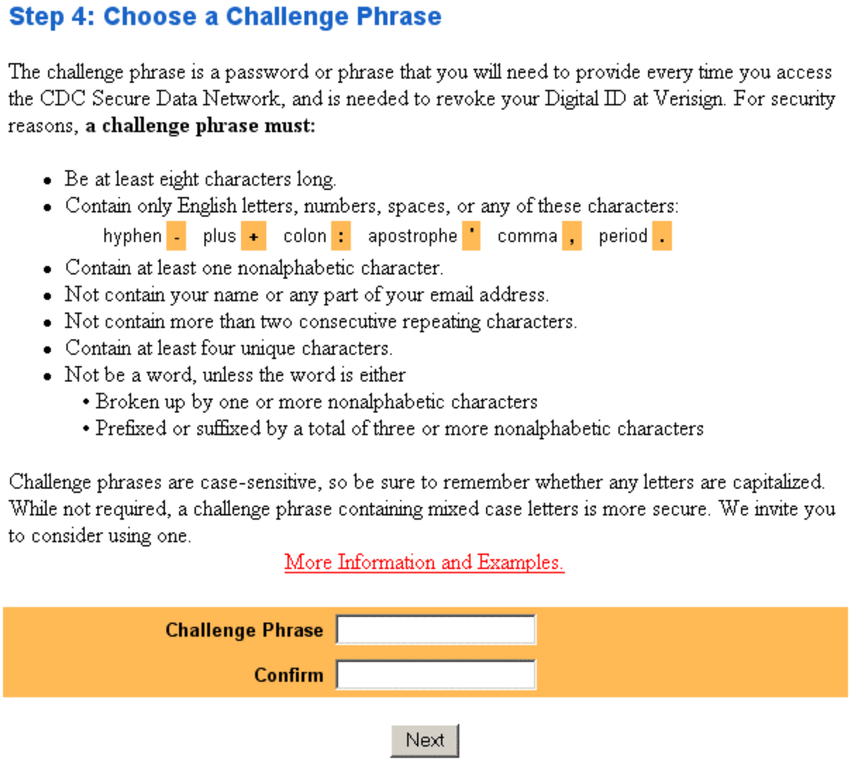
Step 3: Select Smallpox Vaccination Program Activities

Select one or more activities from the list.

Help and Questions and Answers
Semi-Weekly Progress Reporting
Vaccine Administration Support (PVS)

Slide 26

12. Step 4 - Choose a Challenge Phrase: A challenge phrase is required for use and management of your digital certificate. You must select a challenge phrase based on the guidelines presented and enter it twice (once in the "Challenge Phrase" field and once in the "Confirm" field). After your challenge phrase has been entered in both fields, click the NEXT button to continue.



Step 4: Choose a Challenge Phrase

The challenge phrase is a password or phrase that you will need to provide every time you access the CDC Secure Data Network, and is needed to revoke your Digital ID at Verisign. For security reasons, **a challenge phrase must:**

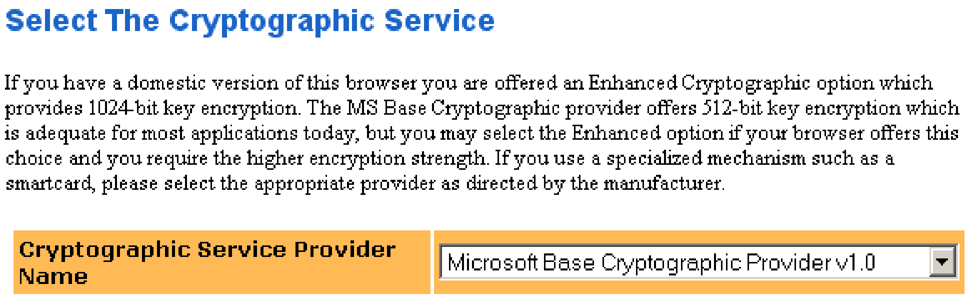
- Be at least eight characters long.
- Contain only English letters, numbers, spaces, or any of these characters:
  hyphen - plus + colon : apostrophe ' comma , period .
- Contain at least one nonalphabetic character.
- Not contain your name or any part of your email address.
- Not contain more than two consecutive repeating characters.
- Contain at least four unique characters.
- Not be a word, unless the word is either
  - Broken up by one or more nonalphabetic characters
  - Prefixed or suffixed by a total of three or more nonalphabetic characters

Challenge phrases are case-sensitive, so be sure to remember whether any letters are capitalized. While not required, a challenge phrase containing mixed case letters is more secure. We invite you to consider using one.

More Information and Examples.

Slide 27

13. Select a cryptographic service provider (CSP) and priority
14. The Cryptographic Service Provider (CSP) is used to generate the digital certificate and determines the "cipher strength" employed. Due to the fact that greater cipher strength is more desirable for transaction security, you should choose the strongest CSP available.
15. The CSP you choose should be based on the following priority (the available CSPs may vary):
    a) Microsoft Strong Cryptographic Provider
    b) Microsoft Enhanced Cryptographic Provider
    c) Microsoft Basic Cryptographic Provider



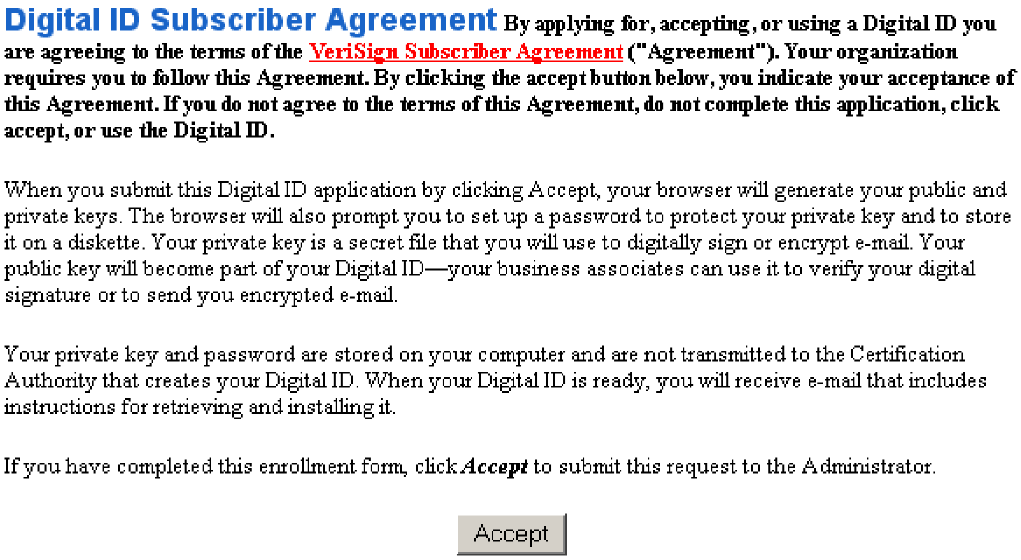
Select The Cryptographic Service

If you have a domestic version of this browser you are offered an Enhanced Cryptographic option which provides 1024-bit key encryption. The MS Base Cryptographic provider offers 512-bit key encryption which is adequate for most applications today, but you may select the Enhanced option if your browser offers this choice and you require the higher encryption strength. If you use a specialized mechanism such as a smartcard, please select the appropriate provider as directed by the manufacturer.

Cryptographic Service Provider Name: Microsoft Base Cryptographic Provider v1.0

Slide 28

16. After choosing your CSP, you are required to review and accept the VeriSign Subscriber Agreement prior to the issuance of your digital certificate. The issuance and use of a digital certificate from VeriSign is governed by the VeriSign Certification Practice Statement (CPS).
17. Review and accept the VeriSign Subscriber Agreement prior to the issuance of your digital certificate.



Digital ID Subscriber Agreement **By applying for, accepting, or using a Digital ID you are agreeing to the terms of the VeriSign Subscriber Agreement ("Agreement"). Your organization requires you to follow this Agreement. By clicking the accept button below, you indicate your acceptance of this Agreement. If you do not agree to the terms of this Agreement, do not complete this application, click accept, or use the Digital ID.**

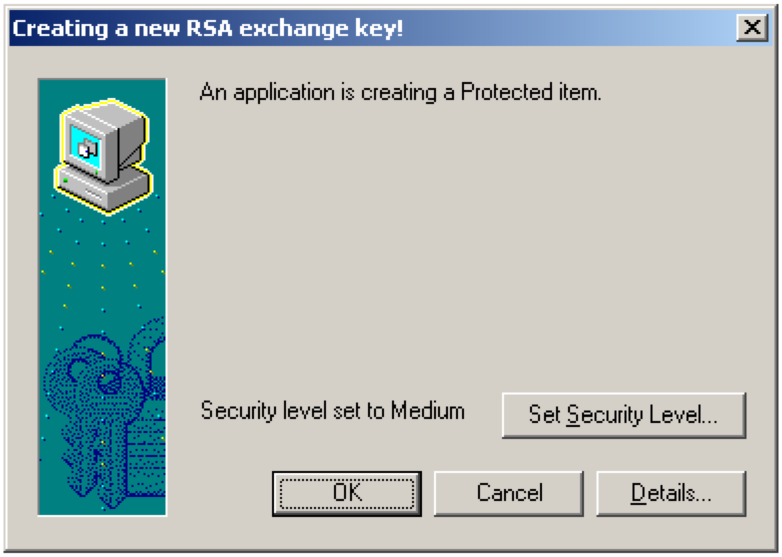
When you submit this Digital ID application by clicking Accept, your browser will generate your public and private keys. The browser will also prompt you to set up a password to protect your private key and to store it on a diskette. Your private key is a secret file that you will use to digitally sign or encrypt e-mail. Your public key will become part of your Digital ID—your business associates can use it to verify your digital signature or to send you encrypted e-mail.

Your private key and password are stored on your computer and are not transmitted to the Certification Authority that creates your Digital ID. When your Digital ID is ready, you will receive e-mail that includes instructions for retrieving and installing it.

If you have completed this enrollment form, click ***Accept*** to submit this request to the Administrator.

Slide 29

18. To begin the process of creating a digital certificate on your computer, it is necessary to generate a key request for submission to the certification authority (CA).
19. Upon acceptance of the VeriSign Subscriber Agreement, Internet Explorer attempts to create a placeholder for the digital certificate. This placeholder is used to store information about the digital certificate request and allows the user to set a security level associated with use of the digital certificate.
20. As part of the notification dialog, a security level setting is displayed. To change the security level to one other than that displayed by the dialog, click the SET SECURITY LEVEL button.
    a) High – Internet Explorer prompts the user prior to use of the digital certificate and requires a password to be entered (this password may be different than the challenge phrase).
    b) Medium – Internet Explorer prompts the user prior to the use of the digital certificate.
    c) Low – Internet Explorer automatically uses the digital certificate without prompting the user.



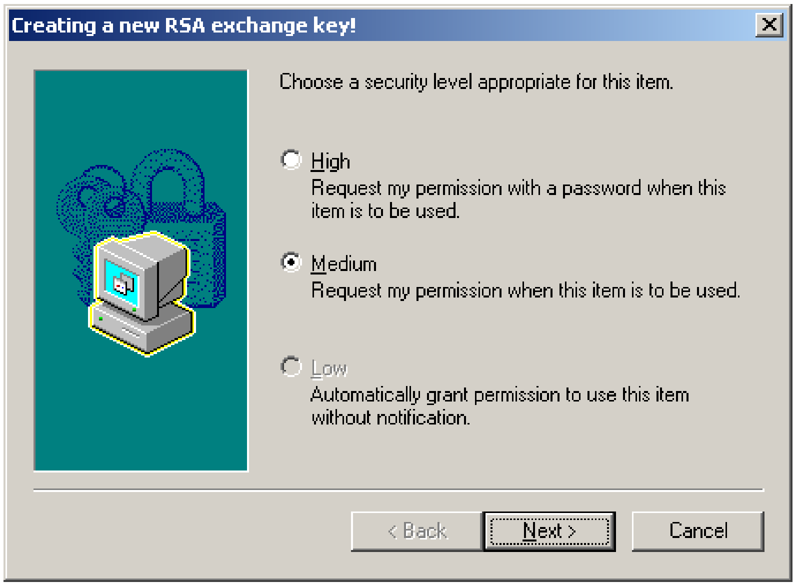
Creating a new RSA exchange key!

An application is creating a Protected item.

Security level set to Medium

Slide 30

21. A dialog in which the available security levels are presented will appear. Click the NEXT button to continue.



Creating a new RSA exchange key!

Choose a security level appropriate for this item.

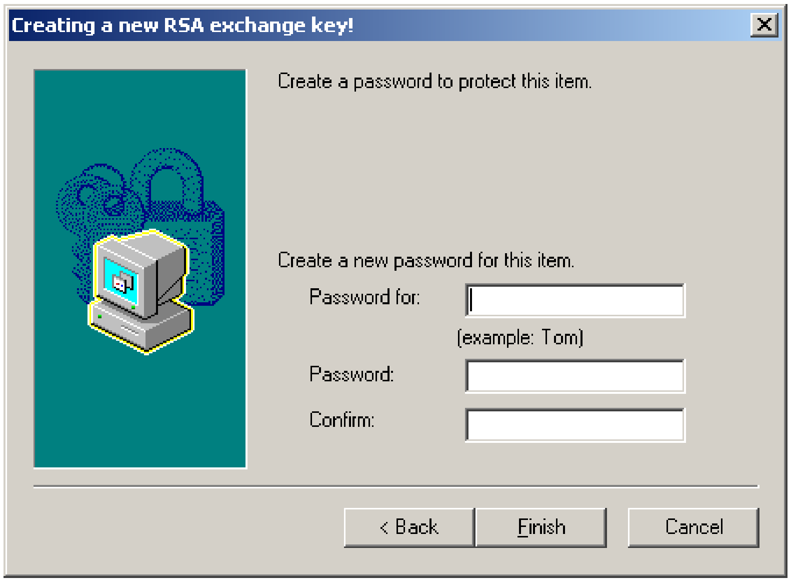
○ High
Request my permission with a password when this item is to be used.

● Medium
Request my permission when this item is to be used.

○ Low
Automatically grant permission to use this item without notification.

Slide 31

22. If the security level is set to "High", a password dialog will appear.



Creating a new RSA exchange key!

Create a password to protect this item.

Create a new password for this item.

Password for:

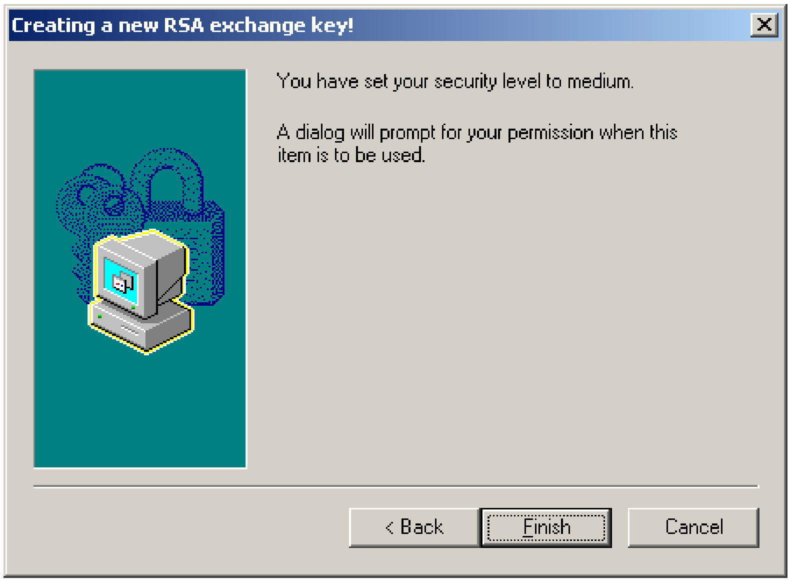
(example: Tom)

Password:

Confirm:

Slide 32

23. If the security level is set to "Medium", a confirmation dialog will appear.



Creating a new RSA exchange key!

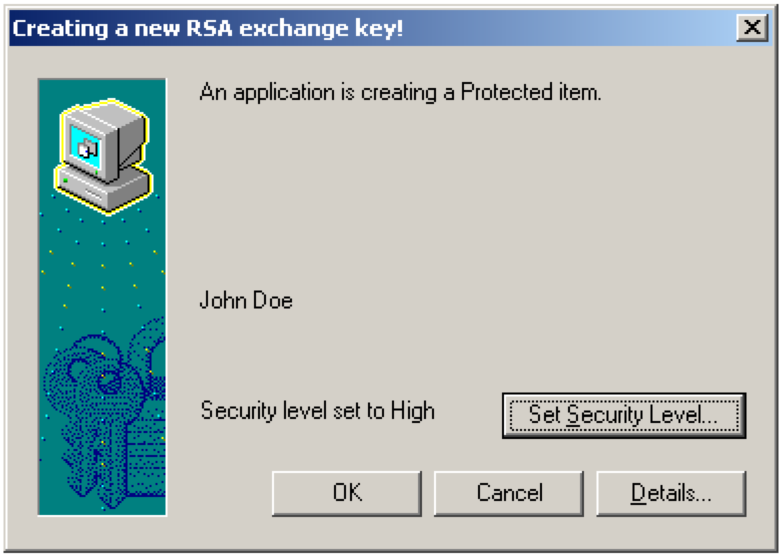
You have set your security level to medium.

A dialog will prompt for your permission when this item is to be used.

24. If the security level is correct, click the FINISH button to continue. If the security level is not correct, click the BACK button to return to the security level selection dialog. After setting the security level, the original notification dialog reappears and reflects any security level changes made.

Slide 33

25. If the security level settings are correct, click the OK button to continue.



Creating a new RSA exchange key!

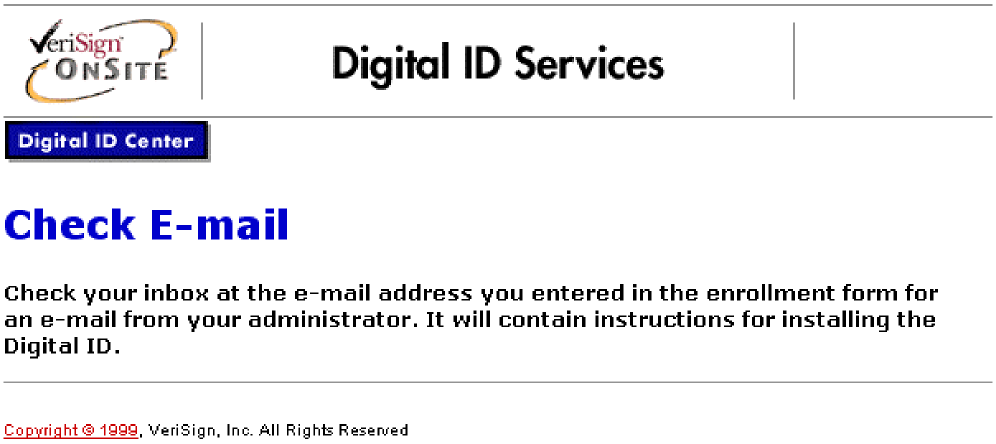
An application is creating a Protected item.

John Doe

Security level set to High

Slide 34

26. Once the digital certificate placeholder has been created, a notification to check your Email account (the one provided during enrollment) will appear.



Check E-mail

Check your inbox at the e-mail address you entered in the enrollment form for an e-mail from your administrator. It will contain instructions for installing the Digital ID.

Copyright © 1999, VeriSign, Inc. All Rights Reserved

27. An Email will be sent to your account with instructions and a personal identification number (PIN) for obtaining your digital certificate.
28. The digital certificate will be distributed 1-2 business day after submitting the digital certificate request.

Slide 35

VII. Installing the Digital Certificate

PVS Training

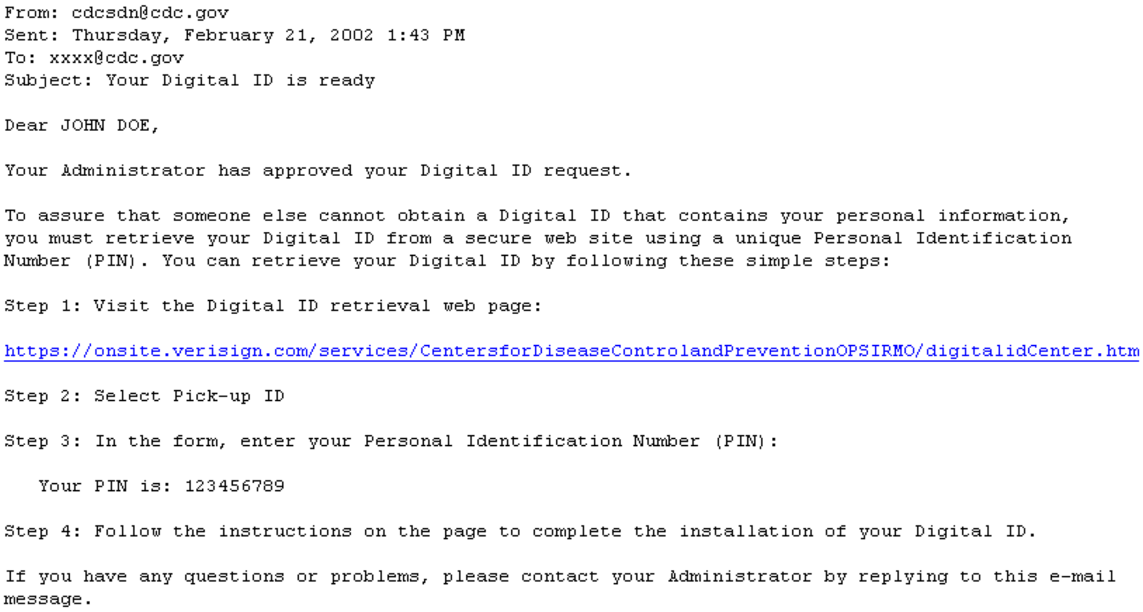
Installing the Digital Certificate

35

Slide 36

A. Please note, you must use the same computer and browser to pick-up your digital certificate as was used to complete the enrollment process. If a different browser or computer is used, the installation will fail.

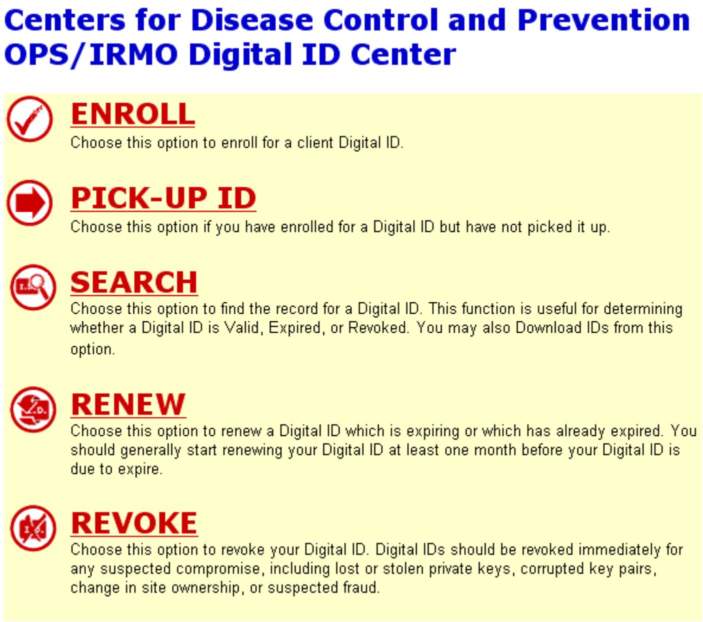
B. To complete the installation of your digital certificate, go the URL provided in the Email notification.



```
From: cdcsdn@cdc.gov
Sent: Thursday, February 21, 2002 1:43 PM
To: xxxx@cdc.gov
Subject: Your Digital ID is ready

Dear JOHN DOE,

Your Administrator has approved your Digital ID request.

To assure that someone else cannot obtain a Digital ID that contains your personal information,
you must retrieve your Digital ID from a secure web site using a unique Personal Identification
Number (PIN). You can retrieve your Digital ID by following these simple steps:

Step 1: Visit the Digital ID retrieval web page:

https://onsite.verisign.com/services/CentersforDiseaseControlandPreventionOPSIRMO/digitalidCenter.htm

Step 2: Select Pick-up ID

Step 3: In the form, enter your Personal Identification Number (PIN):

   Your PIN is: 123456789

Step 4: Follow the instructions on the page to complete the installation of your Digital ID.

If you have any questions or problems, please contact your Administrator by replying to this e-mail
message.
```

Slide 37

C. The notification URL will direct the browser to the VeriSign Digital ID Center for CDC.



Centers for Disease Control and Prevention
OPS/IRMO Digital ID Center

ENROLL
Choose this option to enroll for a client Digital ID.

PICK-UP ID
Choose this option if you have enrolled for a Digital ID but have not picked it up.

SEARCH
Choose this option to find the record for a Digital ID. This function is useful for determining whether a Digital ID is Valid, Expired, or Revoked. You may also Download IDs from this option.

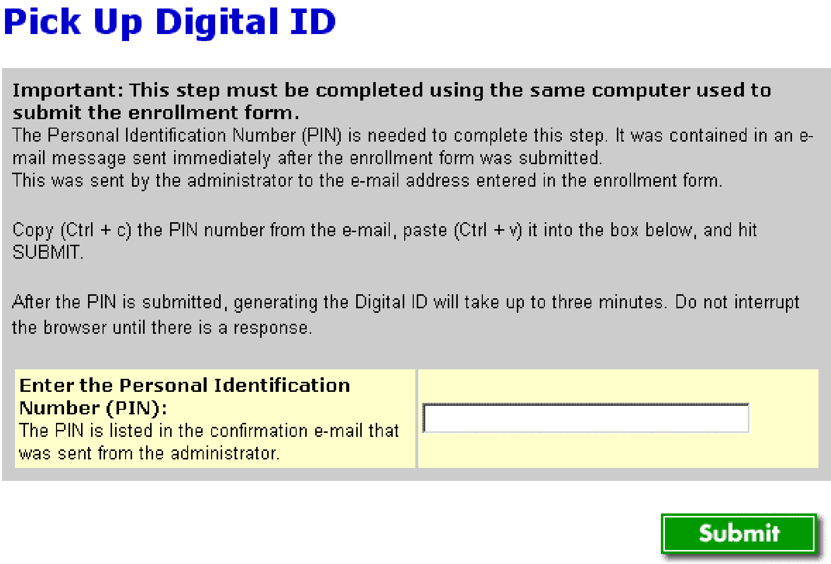
RENEW
Choose this option to renew a Digital ID which is expiring or which has already expired. You should generally start renewing your Digital ID at least one month before your Digital ID is due to expire.

REVOKE
Choose this option to revoke your Digital ID. Digital IDs should be revoked immediately for any suspected compromise, including lost or stolen private keys, corrupted key pairs, change in site ownership, or suspected fraud.

Slide 38

D. To obtain the digital certificate, click on the PICK-UP ID option from the menu. A form will appear that requires the PIN sent in the notification Email.

E. Once the PIN has been entered, click the SUBMIT button to download the digital certificate.



Pick Up Digital ID

Important: This step must be completed using the same computer used to submit the enrollment form.
The Personal Identification Number (PIN) is needed to complete this step. It was contained in an e-mail message sent immediately after the enrollment form was submitted.
This was sent by the administrator to the e-mail address entered in the enrollment form.

Copy (Ctrl + c) the PIN number from the e-mail, paste (Ctrl + v) it into the box below, and hit SUBMIT.

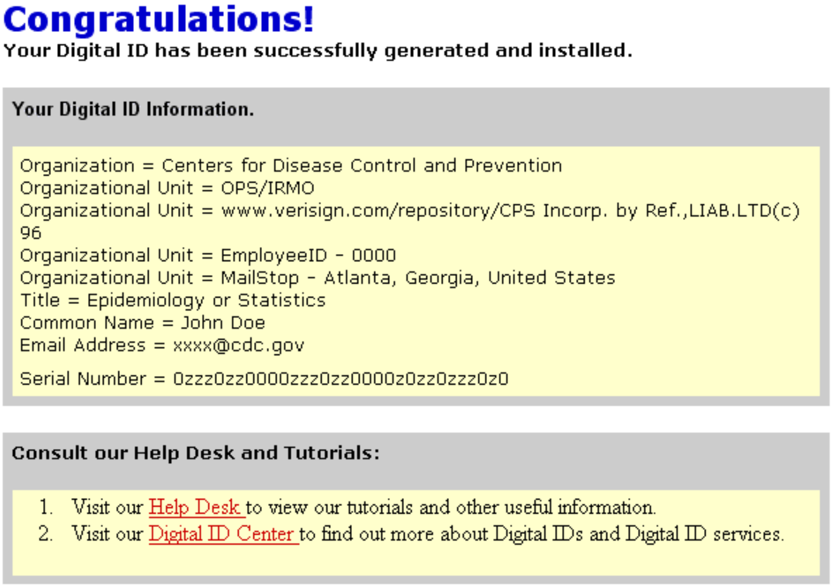
After the PIN is submitted, generating the Digital ID will take up to three minutes. Do not interrupt the browser until there is a response.

Enter the Personal Identification Number (PIN):
The PIN is listed in the confirmation e-mail that was sent from the administrator.

Slide 39

F. If the digital certificate has been successfully installed, a confirmation page with the details of the certificate will be displayed.

G. The information contained in the confirmation page should not be printed or disclosed—it is for verification purposes only. The information presented can be referenced by viewing the details of the digital certificate from the browser.



Congratulations!

Your Digital ID has been successfully generated and installed.

Your Digital ID Information.

Organization = Centers for Disease Control and Prevention
Organizational Unit = OPS/IRMO
Organizational Unit = www.verisign.com/repository/CPS Incorp. by Ref.,LIAB.LTD(c) 96
Organizational Unit = EmployeeID - 0000
Organizational Unit = MailStop - Atlanta, Georgia, United States
Title = Epidemiology or Statistics
Common Name = John Doe
Email Address = xxxx@cdc.gov

Serial Number = 0zzz0zz0000zzz0zz0000z0zz0zzz0z0

Consult our Help Desk and Tutorials:

1. Visit our Help Desk to view our tutorials and other useful information.
2. Visit our Digital ID Center to find out more about Digital IDs and Digital ID services.

Slide 40

VIII. Step 1: Digital Certificate Login

PVS Training

Step 1: Digital Certificate Login

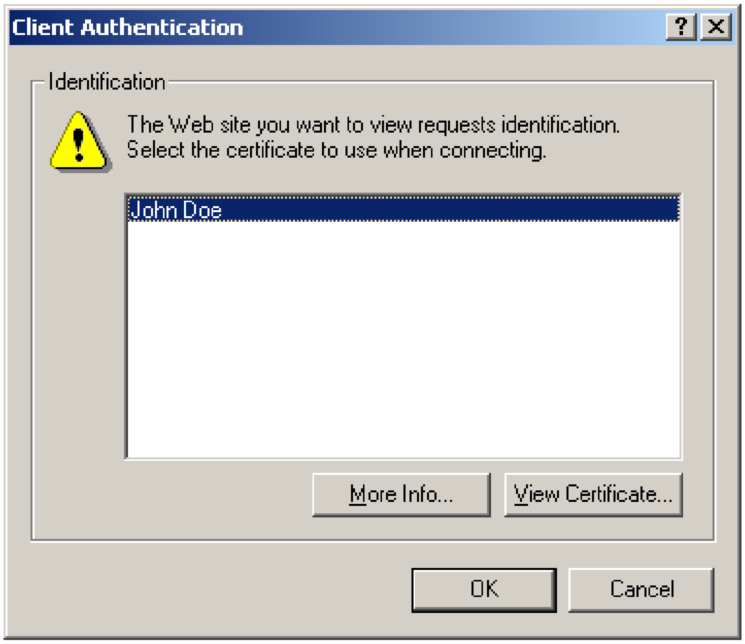
40

Slide 41

Accessing the SDN system:

A. After obtaining and installing the digital certificate, the SDN website can be accessed by going to the following URL: https://sdn.cdc.gov

B. Depending upon the security level of the digital certificate used to access SDN, a user prompt may appear.



Client Authentication

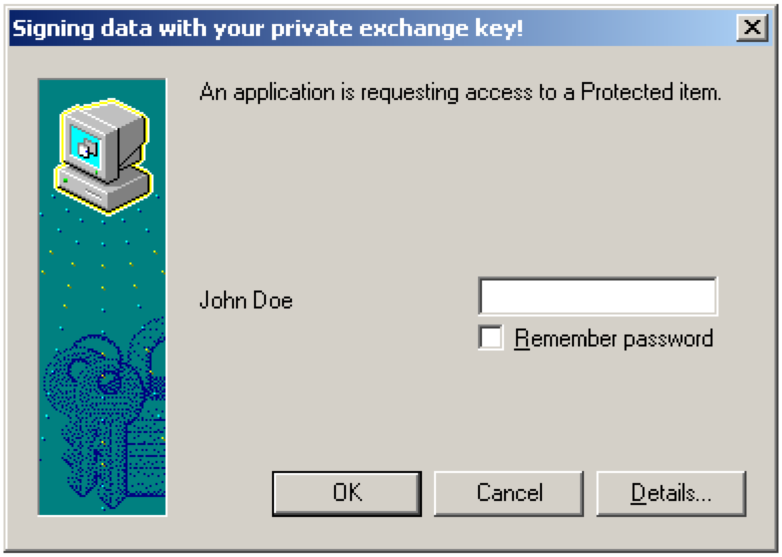
Identification

The Web site you want to view requests identification. Select the certificate to use when connecting.

John Doe

Slide 42

C. Verify the correct digital certificate is being used and click the OK button to continue. If a password is required for use of the digital certificate, a second prompt will appear.



Signing data with your private exchange key!

An application is requesting access to a Protected item.

John Doe

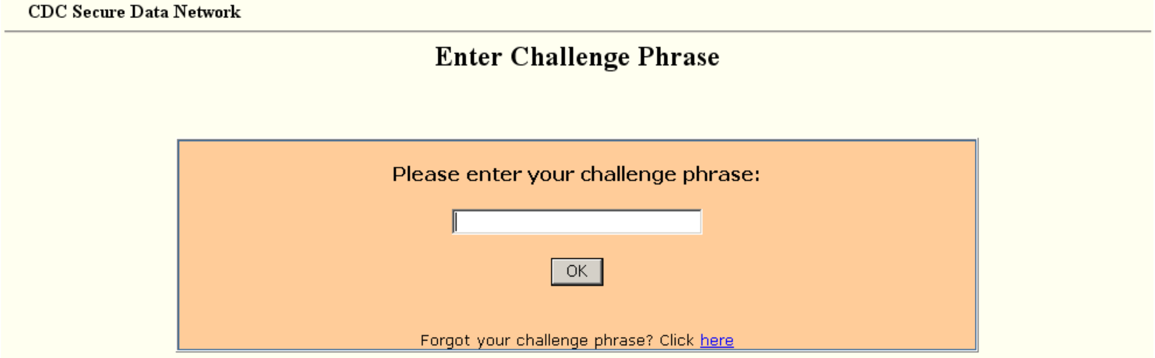
□ Remember password

D. The password assigned to the digital certificate (not the SDN challenge phrase, unless the same password was used) must be entered. After entering the password, click the OK button to continue.

Slide 43

E. After prompting and/or authentication of the digital certificate, the SDN challenge phrase screen will be presented.

F. After entering the password, click the OK button to continue.



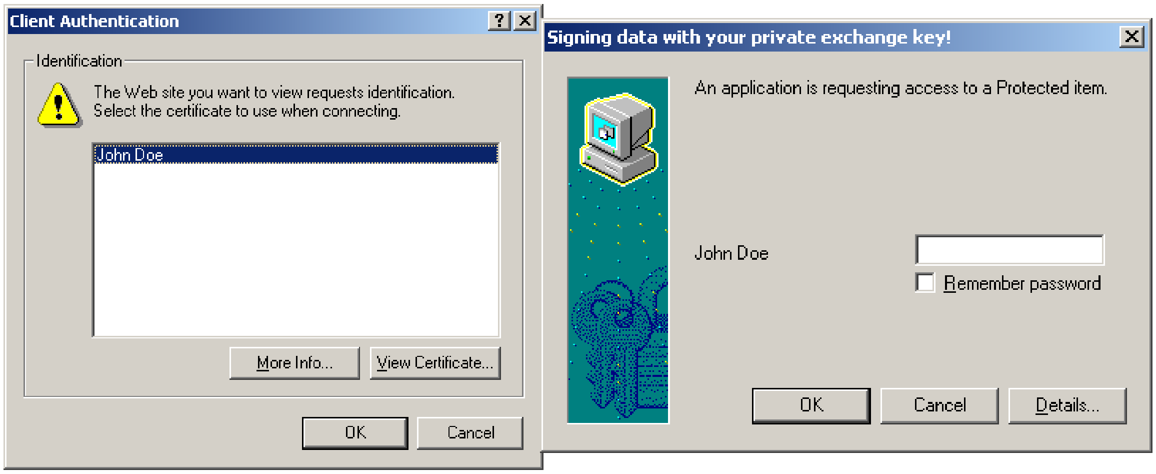
CDC Secure Data Network

Enter Challenge Phrase

Please enter your challenge phrase:

Forgot your challenge phrase? Click here

G. Click OK on the Client Authentication and Signing Data with you Private Exchange Key screens to continue.



Client Authentication

Identification

The Web site you want to view requests identification. Select the certificate to use when connecting.

John Doe

Signing data with your private exchange key!

An application is requesting access to a Protected item.

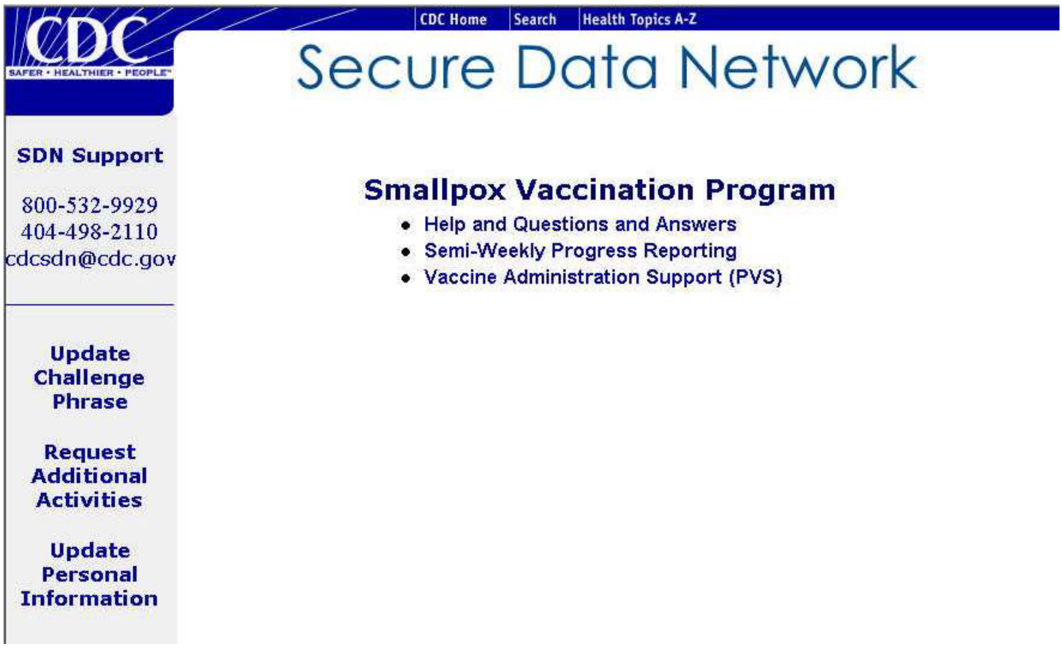
John Doe

□ Remember password

Slide 44

H. Once the challenge phrase has been verified, the main SDN page will be displayed providing a list of all available activities.

I. Select Vaccine Administration Support (PVS) to access the PVS application.



Secure Data Network

SDN Support

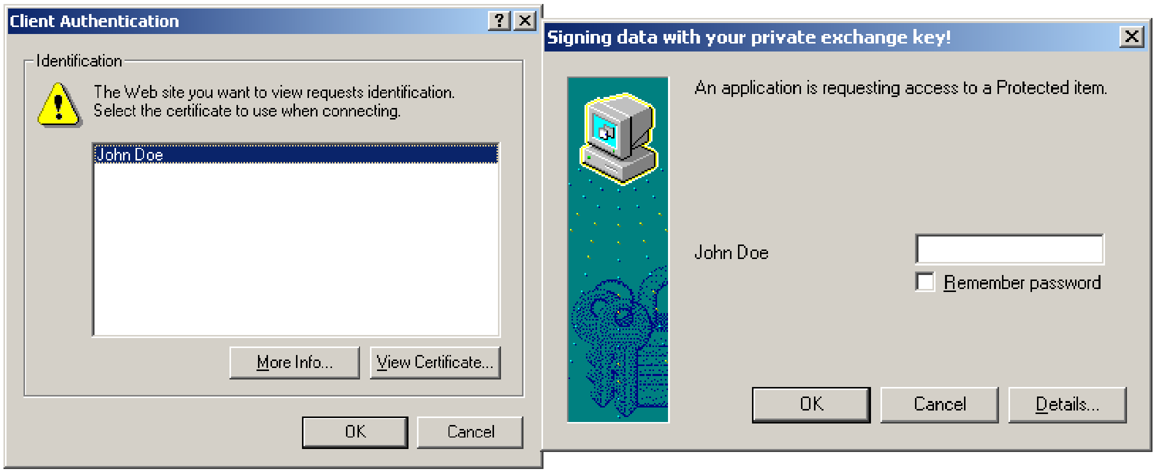
800-532-9929
404-498-2110
cdcsdn@cdc.gov

Smallpox Vaccination Program

- Help and Questions and Answers
- Semi-Weekly Progress Reporting
- Vaccine Administration Support (PVS)

CDC
SAFER • HEALTHIER • PEOPLE
CDC Home
Search
Health Topics A-Z
Update Challenge Phrase
Request Additional Activities
Update Personal Information

J. Click OK on the Client Authentication and Signing Data with you Private Exchange Key screens to continue.



Client Authentication

Identification

The Web site you want to view requests identification. Select the certificate to use when connecting.

John Doe

Signing data with your private exchange key!

An application is requesting access to a Protected item.

John Doe

□ Remember password