

Развертывание центра сертификации на базе Windows Server 2003



Содержание

1.	Общая информация	3
2.	Установка IIS-сервера (Application Server)	3
3.	Установка Certification Authority (CA)	4
4.	Создание и управление сертификатами	5
4.	Установка корневого сертификата	6
5.	Настройка групповых политик	9
5.	Запрос сертификата контроллера домена	10
6.	Включение контроллера домена в группу CERTSVC_DCOM_ACCESS	10
7.	Настройки безопасности	13
8.	Разрешение на запрос сертификатов	15
9.	Процесс выдачи сертификата пользователя	17
6.	Установка ESMART PKI Client	20



1. Общая информация

В руководстве описана настройка службы сертификатов Active Directory на базе Windows Server 2003¹.

Настройка служб каталогов Active Directory не рассматривается. Для выполнения описанных процедур требуются права администратора домена (группа Domain Admin) или администратора предприятия (группа Enterprise Admin).

Собственный корпоративный центр сертификации² может быть развернут на базе Windows Server 2003. Корпоративный центр сертификации позволяет выпускать сертификаты по шаблонам, используя информацию о пользователях из Active Directory. Центр сертификации на базе Windows Server 2003 имеет веб-интерфейс, который может использоваться для запроса сертификата и записи на смарткарту или USB-ключ ESMART Token.

Microsoft не рекомендует разворачивать центр сертификации на сервере, являющимся контроллером домена, желательно использовать другую машину.

2. Установка IIS-сервера (Application Server)

🐻 Add or Remove Programs	
Windows Components Wizard	
Windows Components You can add or remove components of Windows.	CD or <u>Floppy</u>
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.	nternet, click Windows Update
<u>Components:</u>	Category: All Categories
🗹 📻 Accessories and Utilities 4.9 MB 🔺	
Active Directory Services 16.7 MB	
🗹 🕞 Application Server 34.4 MB	
🗹 📴 Certificate Services 1.8 MB	
🗖 🔍 Distributed Eile System 👘 🕺 🕺	
Description: Includes ASP.NET, Internet Information Services (IIS), and the Application Server Console.	
Total disk space required: 15.1 MB Details Space available on disk: 18096.4 MB	
< <u>B</u> ack <u>N</u> ext > Cancel Help	

Убедитесь, что достаточно места для установки и нажмите **Next** (Далее). Дождитесь завершения установки. Закройте программу установщик, нажав **Finish** (Готово).

² Перевод термина Certification Authority соответствует текущей локализации OC Windows Server



¹ С особенностями поддержки функций службы сертификатов Active Directory в разных версиях операционной системы Windows Server 2008 можно на сайте Microsoft: <u>http://technet.microsoft.com/ru-ru/library/cc755071.aspx</u>

3. Установка Certification Authority (CA)

	<u> </u>
Add a program from CD-ROM or floppy disk Change or Remove Windows Components Wizard Windows Components Wizard	
Add program Add program Select the type of CA you want to set up.	
Add yew programs Add program Add/Remove Windows components Enterprise subordinate CA Stand-alone subordinate CA Stand-alone subordinate CA Description of CA type The most trusted CA in an enterprise. Should be installed before any other CA. Use custom settings to generate the key pair and CA certificate Eack Next > Cancel Help 	

Заполните форму, указав название, суффикс и срок истечения корневого сертификата:

Windows Components Wizard				×
CA Identifying Information Enter information to identify th	is CA.			Ē
Common name for this CA:				
test				
Distinguished name suffix:				
DC=testdomain,DC=test				
Preview of distinguished name:				
CN=test,DC=testdomain,DC=test				
⊻alidity period: 5 Years ▼		Expiration da 3/12/2016 4	te: :25 PM	
	< <u>B</u> ack	<u>N</u> ext >	Cancel	Help

Примерно, срок действия сертификата УЦ должен быть в 2-5 раз больше, чем срок сертификатов, которые будет выписывать данный УЦ.



Выберите папку, в которой будет храниться база данных и логи базы:

Windows Components Wizard	×
Certificate Database Settings Enter locations for the certificate database, database log, and configura information.	ation
Certificate database:	
C:\WINDOWS\system32\CertLog	Br <u>o</u> wse
Certificate <u>d</u> atabase log:	
C:\WINDOWS\system32\CertLog	Bro <u>w</u> se
Store configuration information in a shared folder Shared folder:	
	Browse
Preserve existing certificate database	
< <u>B</u> ack <u>N</u> ext > Cance	Help

Нажмите Next (Далее). Подтвердите установку роли.

Центр сертификации установлен.

4. Создание и управление сертификатами

Для управления сертификатами через web-интерфейс можно зайти на страницу<u>http://serv/certsrv</u> или <u>http://localhost/certsrv</u> на самом сервере.

Доступ для управления сертификатами возможен только из браузера Internet Explorer и OC Windows XP (или Windows Server на самом сервере). Элементы управления Active X должны быть установлены и активны.

В веб-интерфейсе СА можно:

- Запросить сертификат (Request a certificate);
- Просмотреть статус запрошенных, но не одобренных сертификатов
- (View the status of a pending certificate request), используется, только если пользователи могут сами запрашивать сертификаты;
- Скачать корневой сертификат CA, серию сертификатов или список отозванных сертификатов (Download a CA certificate, certificate chain or CRL).



🚰 Microsoft Certificate Services - Microsoft Internet Explorer		_ 8 ×
File Edit View Favorites Iools Help		1
🔇 Back 🔻 🕤 👻 📓 🏠 🔎 Search 👷 Favorites 🤣 😓		
Address 🚳 http://localhost/certsrv/	🗲 Go	Links »
<i>Microsoft</i> Certificate Services test	<u>Ho</u>	me.
Welcome		_
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By us certificate, you can verify your identity to people you communicate with over the Web, sign and encryp messages, and, depending upon the type of certificate you request, perform other security tasks. You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, o certificate revocation list (CRL), or to view the status of a pending request.	sing a xt r	K
For more information about Certificate Services, see <u>Certificate Services Documentation</u> .		
Select a task: <u>Request a certificate</u> <u>View the status of a pending certificate request</u> <u>Download a CA certificate, certificate chain, or CRL</u>		
l 🖉 🛛 🗍 🗍 📢 Local ir	ntranet	

4. Установка корневого сертификата

Для получения корневого сертификата выберите нижнюю ссылку: Download a CA certificate, certificate chain or CRL

На странице certcarc.asp выберите корневой сертификат по названию, заданному в поле Common пате на этапе 2. Укажите метод кодирования. DER используется для совместимости с другими ОС, Base64 предназначен для работы с протоколом S/MIME.

Microsoft Certificate Services - Microsoft Internet Explorer		_ 8 ×
Eile Edit <u>Y</u> iew F <u>a</u> vorites <u>T</u> ools <u>H</u> elp		- -
3 Back 🔻 🕤 🔻 😰 🏠 🔎 Search 👷 Favorites 🧀 😓 🔜		
Address 🙆 http://localhost/certsrv/certcarc.asp	🔁 Go	Links [×]
Wicrosoft Certificate Services test	<u>Ho</u>	me
Download a CA Certificate, Certificate Chain, or CRL		_
To trust certificates issued from this certification authority, install this CA certificate chain.		
To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method		
CA certificate:		
Current [test]		
Encoding method:		
© DER		
C Base 64		
Download CA certificate		
Download CA certificate chain		
Download latest base CRL		
Download latest delta CRL		



В появившемся окне нажмите **Ореп** (Открыть):



Сертификат откроется в новом окне. Нажмите Install Certificate (Установить сертификат):

e١	Microsoft Certificate Services - Microsoft Internet Explorer		ζ
E	Certificate ? 🗙		
G	General Details Certification Path		
Aç		Go Links	>
	Certificate Information		
Ч	This certificate is intended for the following purpose(s):	<u>Home</u>	
r.	•All issuance policies		
1	All application policies		
		stall this CA certificate chain.	
-		et the cortificate and encoding method	
		ct the certificate and encoding method.	
2	Issued to: test		
	Iccued by: test		
	issued by. test		
	Valid from 3/12/2011 to 3/12/2016		
E			
1			
	Issuer Statement		
]			
]	OK]	
	ownload latest base CRL		
L	ownload latest delta CRL	_	
_			

Появится окно помощника для импорта сертификата:



Выберите место хранения сертификата:

- Автоматически выбрать хранилище в зависимости от типа сертификата (Рекомендуется)
- Помещать все сертификаты в определенную папку (для опытных пользователей)

Нажмите	Next	(Далее).
---------	------	----------

tificate Store					
Certificate stores a	are system areas w	here certific	ates are kep	ot.	
Windows can autor	matically select a c	ertificate sto	re, or you c	an specif	y a location fo
Automatical	ly select the certifi	cate store ba	ased on the	type of c	ertificate
C Place all cert	tificates in the follo	wing store			
Certificate s	tore:	-			
					Browse
,					

При установке корневого сертификата требуется выбрать хранилище «Доверенные корневые сертификаты вручную.

Проверьте выбранные опции хранилища и тип содержимого. Нажмите Finish (Готово).



5. Настройка групповых политик

line the contract of the contr	mputers	
🎻 Eile <u>A</u> ction <u>V</u> iew <u>W</u> indow	Help	_8×
← → 🗈 💽 🖀 😭 📀	B 🖻 💷 🦉 🖉 边 🖓 🍕 🗑	
 ← → È Active Directory Users and Computers Saved Queries Estdomain.test Estdomain Controllers ForeignSecurityPrive Users 	Image: Second	tainer for upgr tainer for dom tainer for secu tainer for upgr
•	OK Cancel Apply	

Необходимо импортировать доменный сертификат, если его нет в хранилище.



5. Запрос сертификата контроллера домена

	putery/rersonal/i	.eruncacesj			
B Eile Action View Favorites Window Help					×
Console Root	Issued To 🛛 🛆		Issued By		Expiration Date
Certificate Templates	129b380c8ea2.te	stdomain.test	test		3/13/2012
E 👹 Certificates (Local Computer)	Elest		test		3/12/2016
Certificate Request	Wizard			×	
Trusted Root Certification Certificate Types					
Certificates A certificate ty	pe contains preset p	roperties for certifica	ites.		
Enterprise Trust	F				
Select a certification Select a certification	ate type for your re	quest. You can acce	s only certificate types that	:	
Certificates you have pern	issions for and that	are available from a t	rusted CA.		
Trusted Publishers Certificate typ	es:				
Untrusted Certificates Domain Cont	roller			_	
Certificates					
Trusted People					
Certificate Enrollment Re					
SPC *					
To select a cry	ptographic service p	rovider and a CA, sel	ect Advanced.		
		a Deada			
		< <u>B</u> ack		ncel	
	•				•
Personal store contains 2 certificates.	,				
🐉 Start 🛛 🕝 🙈 👘 🔮 dnsmgmt - [DNS\ 🕅 🗞	Console1 - [Co	active Directory	🕞 🔐 Group Policy Obi	. 🛛 🥭 Micros	oft Certific

6. Включение контроллера домена в группу CERTSVC_DCOM_ACCESS

	2						
Se	left Active Directory Users and Comp	uters					
Conin	GEILE Action View Window He	lp					_8×
	← → 🗈 🖬 👗 🛍 🗙 😭	12 🗟 😫 🖪	II 🦉 💯 🐌 '	7 🍕	1		,
	Active Directory Users and Computer	Domain Contro	illers 1 objects				
	i ⊞	Name		Туре	Descripti	on	
	Builtin Computers Omain Controllers ForeignSecurityPrincipals Users	11586-98380	Reset <u>A</u> ccount Mo <u>v</u> e <u>M</u> anage All Tas <u>k</u> s Cu <u>t</u> Delete	- ompi	ıter		
			– P <u>r</u> operties				
			<u>H</u> elp				
	· ·						
		r					
樻 St	art 🛛 🧭 🦽 🗍 🎻 Active Direc	tory User					

,	
Se	🖗 Active Directory Users and Computers
Confi	G File Action View Window Help
	← → 🗈 📧 👗 😤 ≻ 98380C8EA2 Properties ? 🗙
	General Operating System Member Of Location Member of: Select Groups Select Groups Member of:
a	
40 St	ru j 🥲 🥏 🔤 j 🛷 Active Directory User

Также обязательно нужно добавить нужные шаблоны в оснастке **Certification Authority**:

- Authentificated Session
- Enrollment Agent (Агент подачи заявок)
- Enrollment Agent (Computer)
- Smartcard Logon (Логин по смарт-карте)
- Smartcard User (Пользователь со смарт-картой)

📴 Certification Authority			_ 8 ×				
File Action View Help							
🔯 Certification Authority (Local)	Name	Intended Purpose					
🖃 [📝 test	EFS Recovery Agent	File Recovery					
Revoked Certificates	Basic EFS	Encrypting File System					
Issued Certificates	Domain Controller	Client Authentication, Server Authentication					
	Web Server	Server Authentication					
- Failed Requests	Computer	Client Authoritistion Server Authoritistion					
	le Certificate Templates		<u>? ×</u>				
Select	one or more Certificate Templates to enable	on this Certification Authority					
<u>_</u> 0,000		, on the costine term harrowy					
Nam	a	Intended Purpose					
	nrollment Agent	Certificate Bequest Agent					
E CONTRACTOR E C	nrollment Agent (Computer)	Certificate Request Agent					
200 F	vchange Enrollment Agent (Offline request)	Certificate Request Agent					
	vohange Signature Onlu	Secure Email					
	vchange Liser	Secure Email					
	Nonaingo oson Osec	IP securitu IKE intermediate					
	Sec (Offline request)	IP security IKE intermediate					
Sol B	outer (Offline request)	Client Authentication					
200 C	marteard Logon	Client Authentication Smart Card Logon					
900 C	martcard Logon	Secure Email Direct Authentication, Smart Card Logo	n				
BO T	rust List Signing	Microsoft Trust List Signing					
		ОК	Cancel				
]						
🍠 Start 🛛 🚱 🚙 👘 ি Certif	ication Authority						

После всех проведенных операций нужно принудительно обновить политики:

cmd->gpupdate /force

Перезагрузите сервер.

7. Настройки безопасности

Доменные групповые политики позволяют повысить уровень информационной безопасности системы с использованием ESMART Token при помощи двух основных механизмов:

- Вход в систему только при предъявлении ESMART Token;
- Принудительная блокировка рабочей станции или завершение сеанса при извлечении ESMART Token.

Использовать данные механизмы надежнее всего на уровне доменной групповой политики. Возможности изменения локальных настроек на рабочих станциях описаны в руководстве ESMART Token – Авторизация в домене Windows. Правила, заданные доменной групповой политикой имеют наибольший приоритет и потому рекомендуется использовать именно этот метод.

Если решено ввести вход по обязательному предъявлению ESMART Token, необходимо предусмотреть процедуру выдачи временных сертификатов. Для временного отзыва постоянного сертификата используется опция**Certificate Hold**, т.к. только эта причина позволяет впоследствии вернуть статус действующего сертификату, который был отозван.

Чтобы операционная система могла заблокировать рабочую станцию при извлечении ESMART token, необходимо запустить службу **Smartcard Removal Policy – Политика удаления смарт-карт** (**SCPolicySVC**). В ОС Windows XP служба запущена по умолчанию, а в ОС Windows Vista и выше служба по умолчанию отключена. Если служба не запущена, при извлечении ESMART Token не произойдет никаких изменений при любых настройках.

На контроллере домена откройте консоль ММС. Добавьте оснастку Group Policy Management Editor > Default Domain Policy (или текущую доменную политику). Чтобы служба запускалась автоматически на всех рабочих станциях в домене, откройте в редакторе доменной групповой политики:

Computer Configuration > Windows Settings > Security Settings > System Services

Конфигурация компьютера > Конфигурация Windows > Параметры безопасности > Системные службы

Выставите значение для Smart Card Removal Policy – Automatic.

🗐 Group Policy Management Editor								
File Action View Help								
🗢 🧼 🖄 📷 💥 🛱 🗟 🖬								
Default Domain Policy [SERVER.DOMAIN.LOCA	Service Name 🔺	Startup	Permission					
🖃 👰 Computer Configuration	🙀 Secondary Logon	Not Defined	Not Defined					
	🛱 Secure Socket Tunneling Pr	Not Defined	Not Defined					
⊞ Software Settings ■	🛱 Security Accounts Manager	Not Defined	Not Defined					
Windows Settings	🛱 Server	Not Defined	Not Defined					
Name Resolution Policy	🛱 Shell Hardware Detection	Not Defined	Not Defined					
Scripts (Startup/Shutdown)	🛱 Smart Card	Automatic	Not Defined					
E E Security Settings	Smart Card Removal Policy	Automatic	Configured					
Account Policies	SNMP Trap	Not Defined	Not Defined					
	Software Protection	Not Defined	Not Defined					
	💮 Special Administration Cons	Not Defined	Not Defined					
	SPP Notification Service	Not Defined	Not Defined					
	SQL Active Directory Helper	Not Defined	Not Defined					
	SQL Server (MSSQLSERVER)	Not Defined	Not Defined	-				



В той же консоли перейдите к разделу:

Local Policies > Security Options

Локальные политики > Параметры безопасности

В соответствии с корпоративными требованиями задайте значения для параметров:

Interactive Logon: Require smartcard (Интерактивный вход в систему: Требовать смарт-карту)

Interactive Logon: Smartcard removal behavior

(Интерактивный вход в систему: Поведение при извлечении смарт-карты)

ВНИМАНИЕ! Перед перезагрузкой убедитесь, что администратор предприятия или администраторы домена не потеряют возможность входа в систему из-за настройки, требующей обязательного предъявления смарт-карты. Рекомендуется предварительно создать смарт-карту администратора предприятия или администратора домена, имеющего доступ к управлению групповыми политиками

🗐 Group Policy Management Editor								
File Action View Help								
🗢 🔿 🔰 📷 💥 🗒 📑 🚺 🖬	⊨ ⇒ 🖄 📰 😹 😰 🖬							
Computer Configuration Policies Software Settings Windows Settings Windows Settings Scripts (Startup/Shutdown) Security Settings Account Policies Local Policies Local Policies Local Policies Local Policies Security Options Event Log Event Log File System File System Wired Network (IEEE 802.3 Windows Firewall with Adva	Policy Policy Domain member: Disable machine account password changes Domain member: Maximum machine account password age Domain member: Require strong (Windows 2000 or later) session Interactive logon: Display user information when the session is lo Interactive logon: Do not display last user name Interactive logon: Do not require CTRL+ALT+DEL Interactive logon: Message text for users attempting to log on Interactive logon: Number of previous logons to cache (in case d Interactive logon: Prompt user to change password before expir Interactive logon: Require Domain Controller authentication to un Interactive logon: Smart card removal behavior Microsoft network client: Digitally sign communications (always) Microsoft network client: Send unencrypted password to third-pa Microsoft network server: Amount of idle time required before su	Poli A Not Not Not Not Not Not Not Not Not Not						

Проверьте настройки. Обновите групповые политики в принудительном режиме и перезагрузите сервер.

8. Разрешение на запрос сертификатов

Разрешите текущему пользователю (администратору) запрашивать сертификаты для других пользователей (через консоль – команда **ттс** в командной строке **Win+R**):

Запросите новый сертификат:

🚡 Консоль1 - [Корень консоли\Сертификаты - текущий пользователь\Личные] 🔲 🗖 🔀							
📸 Консоль Действие Вид Избранное Окно Справка							
Сертификаты Сертификаты Поиск сертификатов							
Дове Все задачи Поиск сертификатов Поиск сертификатов							
Вид ► Запросить новый сертификат Вид ► Импорт К							
⊕ Дове ⊕ Новый вид панели задач…							
 							
Справка							
Запросить новый сертификат от центра сертификации (ЦС) в этом доме							

1 1 1 1 1 1	Мастер запроса сертификата	
0	Типы сертификатов Тип сертификата определяет заранее установленные свойства сертификатов.	
6	Выберите тип сертификата для запроса. Доступны только те типы, на которые у вас есть разрешение и которые можно получить от доверенного ЦС. Типы сертификатов:	
	Агент восстановления EFS	
	Вход со смарт-картой Подписывание кода Подписывание списка доверия	
	Для выбора поставщика службы криптографии и ЦС установите флажок "Дополнительно". П Дополнительно	
<		
	< Назад Далее > Отмена	1. (1 1 1

та и по Мастер запроса сертифика		
	Завершение работы мастера запроса сертификатов Работа мастера успешно завершена.	
	Были указаны следующие параметры: Понятное имя <нет> Имя учетной записи admin Имя компьютера TESTXPZ Шаблон сертификата Агент подачи заявок	
	< Назад Готово Отмена	

В результате сертификат администратора, позволяющий ему выписывать сертификаты от имени других пользователей, попадет в хранилище.

🚡 Консоль1 - [Коре	нь консоли\С	ертификаты -	текущий польз	овате ль /Личные \Сертифи	кат		
🛅 Консоль Действие	е Вид Избра	иное Окно С	правка				_ & ×
← →	🖻 🗙 🗗	8 🖻 🗉					
🧰 Корень консоли	Кому выдан	🛆 🕴 Кем выдан	Срок действия	Назначения	Имя	Coc	Шаблон (
🖹 🗐 Сертификаты	🕮 admin	test	14.03.2013	Агент запроса сертификата	<het></het>		Агент под
🖃 🛄 Личные				A.			
🔄 Сертиф							
но доверенны На Поверител							
🛓 🦲 Объект по.							
🖮 🦲 Доверенны							
🖻 📃 Сертифика							
⊞… <u> </u> Сторонние							
⊡ Доверенны □ □ □ Запаски за							
н — <u>—</u> запросы за							
	<			III			>
хранилище Личные соде	ржит 1 сертифик	ат.		_			
🦺 пуск 🔰 🌆	ј Администриров	зание 🛛 🕕 С	harismathics Securit.	🛛 🚡 Консоль1 - [Корень	, RL	🗞 🕡 🕄	🎾 21:16



9. Процесс выдачи сертификата пользователя

Только для Windows Server 2003. Windows сервер 2008 и выше не имеют веб-интерфейса для выдачи сертификатов, необходимо использовать консоль. См. руководство Развертывание центра сертификации Windows Server 2008.

Зайдите в WEB-интерфейс CA (http://serv/certsrv или http://localhost/certsrv на самом сервере) с ПК, на котором установлена Windows XP и Internet Explorer. Проверьте, не отключено ли выполнение элементов управления Active X в браузере

(см. руководство к установленной версии браузера Internet Explorer).

Нажмите **Request a certificate** (Запросить сертификат):

Statement Control to Control Alignet Alignet Control Control	
Microsoft Certificate Services - Microsoft Internet Explorer	
Файл Правка Вид Избранное Сервис Справка	
🚫 Назад 🔹 🕥 🖌 😰 🏠 🔎 Поиск 🤺 Избранное 🤣 🏂 🍓 🔜 🖄	
Adpec: 🖉 http://isbc:8080/certsrv/	Ссылки »
	A
Microsoft Certificate Services isbc	lome
Welcome	
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using	а
certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt	
messages, and, depending upon the type of certificate you request, perform other security tasks.	
You can also use this Web site to developed a certificate authority (CA) certificate certificate shain or	
certificate revocation list (CRI) or to view the status of a pending request	
Contineate revocation hist (crite), or to view the status of a perioding request.	
For more information about Certificate Services, see Certificate Services Documentation.	
Select a task:	
Request a certificate	
View the status of a pending certificate request	
Download a CA certificate, certificate chain, or CRL	
	_
и загрузка с узла: ароистріанк	

Выберите advanced certificate request (Расширенный запрос сертификата):

Microsoft Certificate Services test Home					
Request a Certificate					
Select the certificate type: User Certificate	\$				
Or, submit an <u>advanced certificate request</u> .					

Выберите нижнюю ссылку Запросить сертификат от имени другого пользователя, используя станцию выдачи сертификатов:



Также IE запросит разрешение на установку надстройки для выписки сертификата. Подтвердите установку настройки.

Microsoft Smart Card Enrollment Station - Microsoft Internet Explorer	
Файл Правка Вид Избранное Сервис Справка	🥂 🕹 🖓
🕒 Назад 👻 🕟 – 💌 😰 🏠 🔎 Поиск 🤺 Избранное 🔗 –	😓 🖻 🚳
Адрес: 🙋 http://isbc:8080/certsrv/certsces.asp	💌 芛 Переход 🛛 Ссылки 🌺
Internet Explorer заблокировал небезопасное использование элементов управления Acti отображаться неправильно.	іveX на этом веб-узле. Поэтому страница может 🗙
Microsoft Certificate Services	Home
Smart Card Certificate Enrollment Station	
Enrollment Options:	
Certificate Template: 📘 🗾	
Certification Authority: 🔽	
Cryptographic Service Provider:	
Administrator (No certificate selected)	Select Certificate
User To Enroll:	
(No user selected)	Select User
Status:	
An one of the defendence of the second state o	where Management for the state state and as the
An unexpected ratal error has occurred. The proper version of the A install. You may not have sufficient permissions. Please ack your sy	ctiveA control falled to download and
matain, nou may not have summerit permissions. Fiedse dsk your sy	
р Готово	📃 📃 🧐 Местная интрасеть 💋

Выберите необходимые значения для полей:

Microsoft Certificate Services -- isbc

- Шаблон сертификата (Certificate template);
- *Cepmuфuцupyющuй центр (Certificate authority);*
- Криптопровайдер (Cryptographic Service Provider)³;
- Сертификат администратора, от имени которого будет выписан сертификат (Administrator Signing Certificate).

³ ESMART Token использует надстройку над криптопровайдером Microsoft Base Cryptographic Provider.



<u>Home</u>

🗿 Microsoft Smart Card Enrollment Station - Microsoft Internet Explorer 📃 🔪
Файл Правка Вид Избранное Сервис Справка 🥂
🚱 Назад 🝷 💮 🖌 😰 🏠 🔎 Поиск 👷 Избранное 🤣 🔗 - چ 🔜 🖄
Адрес: 🖗 http://isbc:8080/certsrv/certsces.asp 💽 Переход Ссылки *
Microsoft Certificate Services Home
Smart Card Certificate Enrollment Station
Enrollment Options:
Certificate Template: Пользователь со смарт-картой 💌
Certification Authority: isbo 🔽
Cryptographic Microsoft Base Smart Card Crypto Provider 🔽
Administrator Test Select Certificate
User To Enroll:
Testus@corp.isbc.ru Select User
Status
The smart card is ready. Please press 'View Certificate' to make sure the certificate contains the correct personal information about the user.
View Certificate New User
🖹 🛛 🖉 Надежные узлы

Нажмите **Select User** и выберите пользователя смарт-карты. Убедитесь, что считыватель подключен к ПК и в него вставлена карта. Нажмите **Enroll** (Подать заявку).

В появившемся окне введите ПИН-код пользователя, который был задан при создании профиля на карте и нажмите **Вход в систему**.

Microsoft Certificate Services			<u>Home</u>
Smart Card Certificate E	hrollment	Station	
Enrollment Ontions:			
Certificate Template:	Smart Card P	IN	
Certification Authority:		A P	
Cryptographic Service Provider	<u>کا</u> کا		
Administrator E Signing Certificate:		Select Ce	tificate
User To Enroll:	PIN:	KINISISION	
Γ		OK Cancel Select Use	6
Status:			
Please wait while the user i	s enrolled		

Дождитесь подтверждения:

🗿 Microsoft Smart Card Enrollment Station - Microsoft Internet Explorer
Файл Правка Вид Избранное Сервис Справка
😋 Назад 🝷 📀 🚽 😰 🏠 🔎 Поиск 🤸 Избранное 🧔 🍰 - چ 🚍 🦓
Адрес: 🖗 http://isbc:8080/certsrv/certsces.asp 🔽 🄁 Переход 🛛 Ссылки
Microsoft Certificate Services Home
Smart Card Certificate Enrollment Station
Enrollment Options:
Certificate Template: Пользователь со смарт-картой 💌
Certification Authority: isbc 🔽
Cryptographic Microsoft Base Smart Card Crypto Provider 🗾 🔽
Administrator Test Select Certificate
User To Enroll:
Testus@corp.isbc.ru Select User
Status:
The smart card is ready. Please press 'View Certificate' to make sure the certificate contains the correct personal
information about the user.
View Certificate New User
🕑 🛛 🖉 Надежные узлы

Нажмите View Certificate для просмотра сертификата или New User для запроса сертификата для следующего пользователя.

Сертификат получен и записан на карту. Теперь пользователь может использовать сертификат для авторизации в Windows. При авторизации по сертификату вводить необходимо ПИН-код карты, а не пароль пользователя на ПК.

6. Установка ESMART PKI Client

Рекомендуется установить пользователям бесплатное приложение ESMART PKI Client. При установке ESMART PKI Client через групповые политики необходимо заранее установить для всех пользователей сертификат ISBC в хранилище **Доверенные издатели**. Сертификат можно скопировать из инсталлятора приложения.