

Средство защиты информации от несанкционированного доступа «Блокхост-Сеть 4»

Руководство администратора безопасности Часть 3. Настройка подсистемы управления токенами, ЦС Microsoft CA

Санкт-Петербург, 2024

Аннотация

В документе содержатся сведения об установке и настройке подсистемы управления жизненным циклом токенов средства защиты информации от несанкционированного доступа «Блокхост-Сеть 4» при взаимодействии с центром сертификации Microsoft CA и сервисом каталогов Active Directory, а также сведения о настройке сертификатов, необходимых для функционирования подсистемы.

Содержание

Введен	ие	5
1	Подсистема жизненного цикла токенов	6
2	Настройки на контроллере домена	8
3	Настройки центра сертификации1	2
3.1	Сертификат агента регистрации1	2
3.2	Сертификат пользователя2	2
4	Настройки на сервере «Блокхост-Сеть»3	1
4.1	Выпуск и установка сертификата агента регистрации	1
4.2	Создание профилей в настройках подсистемы	4
4.2.1	Создание профиля Microsoft CA	5
4.2.2	Добавление прокси-клиента для взаимодействия с ЦС4	1
5	Особенности при выпуске токена средствами подсистемы4	7
6	Настройка прозрачного входа в RDGW4	8
7	Настройка входа по сертификатам ЦС Microsoft СА в ОС Linux	9
7.1	Приоритет проверок средств аутентификации при входе4	9
7.2	Ввод рабочей станции ОС Linux в домен AD4	9
7.2.1	Ввод рабочей станции под управлением ОС Альт в домен Active Directory4	9
7.2.2	Ввод рабочей станции под управлением OC Astra Linux в домен Active Directory	1
7.2.3	Ввод рабочей станции под управлением РЕД ОС в домен Active Directory5	3
7.3	Порядок настройки для входа по сертификатам в ОС Linux	5
7.3.1	Экспорт корневого сертификата AD	5
7.3.2 развер [.]	Запуск задачи по настройке входа по сертификату через подсистем тывания	у 7
7.4	Особенности при входе в ОС Альт по сертификатам MS СА	4
7.5	Особенности при входе в ОС Astra Linux с настроенным входом по сертификата 6	м 7
7.6	Удаление сертификата из Active Directory пользователя6	7
7.7	Настройка публикации списка отзыва сертификатов в ОС Linux	8
7.7.1	Настройки центра сертификации6	8
7.7.2	Настройки на контроллере домена	5



7.7.3	Публикация списка отзывов87
7.8 устано	Настройка подключения к домену из консоли управления по протоколу <i>ldaps</i> с вкой ssl-сертификатов
7.8.1	Настройка контроллера домена AD89
7.8.2	Настройка контроллера домена Samba97
7.8.3	Настройка контроллера домена FreeIPA99
7.8.4 управл	Настройки на рабочей станции OC Windows с установленной консолью іения
7.8.5	Настройки на рабочей станции ОС Linux с установленной консолью управления
7.8.6	Проверка работоспособности подключения101
7.8.7	Особенности при настройке AD для подключения по ldaps из OC AstraLinux 1.7
Перече	ень сокращений

Введение

Подсистема управления жизненным циклом токенов предназначена для управления носителями пользователей на протяжении всего жизненного цикла.

Для настройки и установки подсистемы управления жизненным циклом токенов в существующей иерархической структуре уже должны быть развернуты следующие компоненты:

– служба каталога Active Directory;

– центр сертификации (Microsoft Enterprise CA), принадлежащий тому же домену Active Directory, в котором будет развернута подсистема управления жизненным циклом токенов.

Знаки, расположенные на полях руководства, указывают на примечания.

Степени важности примечаний:



Важная информация

Указания, требующие особого внимания.



Дополнительная информация

Указания, позволяющие упростить работу с подсистемой.

1 Подсистема жизненного цикла токенов

Подсистема предназначена для управления устройствами аутентификации пользователей на протяжении всего жизненного цикла и обеспечивает учет токенов в системе, управление токенами и аудит в течении всего жизненного цикла.

Подсистема жизненного цикла токенов поддерживает управление токенами перечисленными в таблице 1.1.

Носитоли	Произродитор	Наименование носителя		
поситель	производитель	поддерживаемые OC Windows	поддерживаемые ОС Linux	
		eToken Pro,		
		aTakan FOCT		
		eToken NG-FLASH,		
eToken	SAO «АЛАДДИН Р.Д.»	eToken NG-FLASH (Java),		
		eloken NG-OTP,		
		eToken NG-OTP (Java),		
		eToken GT (Java),		
		eToken PRO (Java) SC,		
		eToken PRO SC		
		SafeNet eToken 5100,		
	000	SafeNet eToken 5105,		
	«Сертифицированн	SafeNet eToken 5200,		
SafeNet eToken	ые	SafeNet eToken 5205,		
	информационные	SafeNet eToken 7200,		
	системы»	SafeNet eToken 7300,		
		SafeNet eToken 4100		
		Рутокен, Рутокен S,		
Durraway		Рутокен Lite, Рутокен ЭЦП,	Pyloken Juli, Pyloken Juli	
Рутокен	SAO «AKTUB COOT»	Рутокен ЭЦП 2.0, Рутокен ЭЦП	2.0, Pytokeh Juli 2.0 Flash,	
		2.0 Flash, Рутокен ЭЦП 3.0	Рутокен Эціт 3.0	
		JaCarta-2,	JaCarta-2,	
JaCarta	ЗАО «АЛАДДИН	JaCarta PKI,	JaCarta PKI,	
	Р.Д.»	JaCarta PRO	JaCarta PRO	
	000			
	«Интеллектуальные			
eSmart Token	системы	eSmart Token	eSmart Token	
	управления			
	бизнесом»			

Таблица 1.1 – Поддерживаемые подсистемой токены

Для работы с сертификатами на токене в подсистеме жизненного цикла токенов необходимо выполнить определенные настройки на контроллере домена, центре сертификации и в самой подсистеме жизненного цикла токенов.

Если на клиентских ОС Windows не хватает компонентов для отзыва сертификатов. Для корректного функционирования подсистемы под управлением клиентских ОС необходимо поставить обновление «Remote Server Administration Tools» (установка «Remote Server Administration Tools» необходима только для ОС Windows 7, 8.1, 10 (до версии 1903) и включить компонент «Средства служб сертификации»:

– для OC Windows 7 "Remote Server Administration Tools for Windows 7" (<u>https://www.microsoft.com/en-us/download/details.aspx?id=7887</u>);

– для OC Windows 8.1 "Remote Server Administration Tools for Windows 8.1" (https://www.microsoft.com/en-us/download/details.aspx?id=28972);

– для OC Windows 10 до версии 1903 "Remote Server Administration Tools for Windows 10" (<u>https://www.microsoft.com/en-us/download/details.aspx?id=45520</u>).¹

i

При выдаче токена *Рутокен ЭЦП* для входа по сертификату на сервере под управлением OC Linux, вход в OC Windows по такому токену будет невозможен, т.к. производитель не поддерживает данную возможность.

¹ В ОС Windows 10 версии 1903 и выше обновление «Remote Server Administration Tools» уже установлено по умолчанию. Включение компонента **«Средства служб сертификации»** доступно в пункте «Панель управления» → «Программы» → «Включение или отключение компонентов Windows».



Для первоначальной настройки подсистемы жизненного цикла токенов необходимо создать сервисную учетную запись, обладающую достаточными правами для создания сертификата и входящую в группу пользователей домена.



GIS ГАЗИНФОРМ СЕРВИС

Сервисная учетная запись должна принадлежать тому же домену, что и центр сертификации.

Для создания сервисной учетной записи (например, *serviceCA*) откройте окно оснастки *Active Directory – Пользователи и компьютеры (Active Directory Users and Computers)* (рисунок 2.1).

🔁 l 🔂 🔝 = l	Shortcut Tools	Administrative	Tools	
File Home Share	View Manage			^
Copy Paste Cipboard	rtcut Nove Copy to Copy to Copy to Copy to Copy	e New folder	Properties Open	Select all
🍥 🛞 = 🕆 🗟 « All	Control Panel Items Administrative	Tools v	🖒 Search Adm	inistrative Tools
☆ Favorites	Name	Date modified	Туре	Size
Desktop	Terminal Services	22.08.2013 19:39	File folder	
🐌 Downloads	Active Directory Administrative C	Center 22.08.2013 3:50	Shortcut	2 KB
💹 Recent places	Active Directory Domains and Tr	usts 22.08.2013 10:55	Shortcut	2 KB
	😿 Active Directory Module for Wind	dows Po 22.08.2013 10:55	Shortcut	2 KB
👰 This PC 🖉	Retive Directory Sites and Service	22.08.2013 10:55	Shortcut	2 KB
📔 Desktop	Active Directory Users and Comp	outers 22.08.2013 10:55	Shortcut	2 KB
Documents	ADSI Edit	22.08.2013 10:55	Shortcut	2 KB
📕 Downloads	Component Services	22.08.2013 10:57	Shortcut	2 KB
Music	🛃 Computer Management	22.08.2013 10:54	Shortcut	2 KB
Pictures	눩 Defragment and Optimize Drives	22.08.2013 10:47	Shortcut	2 KB
Videos	THCP DHCP	22.08.2013 10:45	Shortcut	2 KB
Local Disk (C:)	🛃 DNS	22.08.2013 10:55	Shortcut	2 KB
💼 Data (D:)	🛃 Event Viewer	22.08.2013 10:55	Shortcut	2 KB
	🚮 Group Policy Management	22.08.2013 10:56	Shortcut	2 KB
📭 Network	🔝 iSCSI Initiator	22.08.2013 10:57	Shortcut	2 KB
DESKTOP-WIN10	🔁 Local Security Policy	22.08.2013 10:54	Shortcut	2 KB
IN 218CA02 ∨	Microsoft Azure Services	24.07.2014 8:02	Shortcut	2 KB

Рисунок 2.1 – Переход к оснастке Active Directory Users and Computers

Окно будет иметь следующий вид:

		Active Directory	Users and Cor	nputers – 🖬 🗙
File Action View Help				
(+ +) 2 🗊 / 🗆 🗙 🗊 G 🕞	🛛 🗊 🔧 🖄 🍸 🔤 🗞			
Image: Second	Name admin admin Allowed RODC Password Replication Group Cent Publishers Cloneable Domain Controllers Cloneable Domain Controllers Denied RODC Password Replication Group DHCP Administrators DHCP Administrators Domain Computers Domain Computers Domain Computers Domain Controllers Domain Controllers Domain Controllers Domain Guests Domain Controllers Domain Controllers Domain Controllers Domain Controllers Domain Controllers Domain Controllers Domain Quest Computers Ders Admins Enterprise Read-only Domain Controllers Guest Noted Admin Group Policy Creator Owners RAS and IAS Servers RAS and IAS Servers Computer Section Controllers Schema Admins Tetuseer WinRMRemoteWMIUsers_ Administrator	Last Nafhe	Type User Security Grou Security Grou User User Security Grou Security Grou Security Grou Security Grou Security Grou Security Grou Security Grou Security Grou Security Grou Security Grou User	Description Members in this group can have their passwords replicated to all read-only domain controllers in the domes of this group are permitted to publish certificates to the directory Members of this group cannot have their passwords replicated to any read-only domain controllers in the Members who have administrative access to the DHCP Service Members in this group cannot have their passwords replicated to any read-only domain controllers in the Members who have administrative access to the DHCP Service MS Administrators Group DNS clients who are permitted to perform dynamic updates on behalf of some other clients (such as DHDesigneted administrators of the domain All workstations and servers joined to the domain All domain guests All domain users Designated administrators of the enterprise Members in this group can modify group policy for the domain Built-in account for guest access to the computer/domain Key Distribution Center Service Account Members of this group are acces remote access properties of users Members of this group are access remote access properties of users Members of this group are Read-Only Domain Controllers in the domain Built-in account for administering the computer/domain Key Distribution Center Service Account Members of this group are access remote access properties of users Members of
	& Administrator Enrollment Agent	adminoff Enrollment Ag	User User	Built-in account for administering the computer/domain

Рисунок 2.2 – Оснастка Active Directory Users and Computers

Создайте организационное подразделение (Organizational Unit — OU) издателей сертификатов для работы с выпуском сертификатов подсистемой жизненного цикла токенов (например, на рисунке 2.3 OU **Special**) и создайте группу издателей сертификатов (например, *CertIssuers*) по щелчку правой кнопки мыши *Создать (New)* — *Группа (Group)*.

Создайте сервисную учетную запись по щелчку правой кнопки мыши **Создать (New)** → **Пользователь (User)**. Отобразится окно для ввода данных создаваемой учетной записи пользователя (рисунок 2.3).

3		Active Director	ry Users and Computers	
File Action View Help				
A A	🛛 🖬 🗏 📚 🐄 🍸 💆 🕯	8		
Active Directory Users and Computers [s18	Name	Last Name	Туре	Description
Saved Queries	🚨 Admin CA		User	
⊿ 🚔 diff.pki	Sectissuers		Security Group - Global	Издатели сертов
þ 🖬 BH	& dl_Enrolment_Agent		Security Group - Domain Local	
Builtin	St g_Enrolment_Agent		Security Group - Global	
Computers	Ne	ew Object - User	x	
Domain Controllers	-			
ForeignSecurityPrincipals				
N B INDEED	Create in: diff.pki/	Special		
b 📑 LostAndFound				
Managed Service Accounts				
Program Data	First name:	Initials:		
Smart Card Logon	Last name:			
3 Special				
Stuff	Full name:			
System				
Test 10 Users	User logon name:			
Test Users		@diff.pki	~	
Users	11	2000		
NTDS Quotas	User logon name (pre-vvindows	2000):		
D IPM Devices	DIFF			
		< Back Next >	Cancel	

Рисунок 2.3 – Создание сервисной учетной записи



Введите все необходимые данные и нажмите Далее (Next).

В появившемся окне введите пароль создаваемой сервисной учетной записи и подтвердите его в соответствующем поле, и установите параметры Запретить смену пароля пользователя (User cannot change password) и Срок действия пароля не ограничен (Password never expires) (рисунок 2.4).

	New Object - User	x
Create in:	diff.pki/Special	
Password: Confirm password: User must change pa User cannot change Password never expl Account is disabled	assword at next logon password res	
	< Back Next > Car	ncel

Рисунок 2.4 – Ввод пароля для создаваемой сервисной учетной записи

Нажмите на кнопку *Готово (Finish)* (рисунок 2.5).





В оснастке *Active Directory – пользователи и компьютеры* щелкните правой кнопкой на имени созданной учетной записи и выберите *Свойства (Properties).*

Перейдите во вкладку **Член групп (Member of)** и проверьте принадлежность учетной записи группе пользователей домена (**Domain Users**) и созданной группе издателей сертификатов (**CertIssuers**, OU **Special**) в соответствии с рисунком 2.6. При необходимости, добавьте учетную запись в данные группы по кнопке **Добавить (Add)**.

Security	Er	vironment	Sessi	ons	Remote c	ontrol
Remote	Desktop Se	arvices Profile		OM+	Attribute	Editor
General	Address	Account	Profile	Telephones	Orga	nization
Published (ertificates	Member Of	Password	Replication	Dial-in	Object
Member o	f:					
Name		Active Directo	bry Domain	Services Fold	ler	
CertIssu	ers	diff.pki/Speci	al			
Add.	. F	Remove				
Add Primary gn Set Prir	. F oup: Do	Remove	o need to c Macintosh is.	thange Primar clients or POS	y group u SIX-compli	nless

Рисунок 2.6 – Вкладка Member of

3 Настройки центра сертификации

3.1 Сертификат агента регистрации

Для выпуска пользовательских сертификатов на токене необходим сертификат, выпущенный по шаблону сертификата агента регистрации. В этом случае администратор может обращаться к центру сертификации для выпуска сертификатов пользователям.

Для создания шаблона запустите консоль центра сертификации с помощью команды *certsrv.msc* в командной строке (рисунок 3.1).



Рисунок 3.1 – Запуск консоли центра сертификации

При возникновении ошибки вида, изображенного на рисунке 3.2, в появившейся консоли центра сертификации по щелчку правой кнопки мыши выберите Перенацелить центр сертификации (Retarget Certification Authority) (рисунок 3.3).



Рисунок 3.2 – Ошибка запуска консоли центра сертификации



File

				Certificate Templates C	Console
Action View	Help	2		Certificate Tem	plates Console
ertificate Templa	ates (s18D	File Action View Help			
	i	certsrv -	[Certificati	ion Authority (Local)]	_ _ X
	File A	Action View Help			
	*				
	Certi	fication Authority /Local Name	7	Description	
	0	View	A:	Certification Authority	
		View P	-		
		Help	-		
	d.	пер			
	_				
	Redirect t	this snapin to manage a different Certification A	uthority		

Рисунок 3.3 – Изменение центра сертификации

В появившемся окне установите параметр *Другим компьютером (Another computer)* (рисунок 3.4) и найдите необходимый центр сертификации (рисунок 3.5).

	Certificatio	n Authority	
Select the computer you wan	nt this snap-in to mana	ge.	
This snap-in will always mar	nage:		
O Local computer: (the c	computer this console	s running on)	
Another computer:			 Browse
only applies if you save	the console.		na na m ro. 1189

Рисунок 3.4 – Выбор центра сертификации



CA	Computer
diff-S18CA02-CA	s18CA02.diff.pki

Рисунок 3.5 – Установка центра сертификации

Окно консоли будет выглядеть следующим образом:

Ga da	certsrv - [0	Certification Authority (Local)\diff-S18CA02-CA\Certificate Templates]	_ 0)
File Action View Help			
(* *) 🖄 🙆 🖉			
Province of the second se	Name Administrator Administrator Besic EFS Computer Copy of Enrollment Agent Directory Email Replication Domain Controller Domain Controller Authentication EFS Recovery Agent Enrollment Agent 4 Different Enrollment Agent 4 Different Enrollment Agent to the form of the	Intended Purpose Microsoft Trust List Signing, Encrypting Encrypting File System Client Authentication, Server Authentic Certificate Request Agent Directory Service Email Replication Client Authentication, Server Authentic File Recovery Certificate Request Agent Certificate Request Agent Certificate Request Agent Certificate Request Agent Smart Card Logon, Client Authenticatio Client Authentication, Smart Card Logon Server Authentication, Smart Card Logon Server Authentication, Sinet Card Logon Server Authentication, Smart Card Logon Server Authentication, Sinet Card Logon Server Authentication Client Authentication Server Authentication Se	

Рисунок 3.6 – Консоль центра сертификации

В левой части окна перейдите в свойства центра сертификации (*Properties*) по щелчку правой кнопки мыши (рисунок 3.7).



م آ	certsrv - [Ce	ertification Authority (Local)\diff-S18CA02-CA]							
File Action View	File Action View Help								
Certification Authorit	y (Local) Name								
△ 🚮 diff-S18CA02-C	All Tasks	Certificates							
Issued Cert	View +	Requests							
Pending Re	Refresh	equests							
Certificate	Export List	te Templates							
	Properties								
	Help								
Opens the properties dialo	og box for the current se	election.							



Перейдите во вкладку **Безопасность (Security)** и по кнопке **Добавить (Add)** добавьте группу издателей сертификатов (рисунок 3.8), в которую входит созданная сервисная учетная запись (в примере, **CertIssuers**).



Extensions	Storage		Certificate Manage		
General	Policy Mod	dule	Б	it Module	
Enrollment Agents	Auditing	Recov	ery Agents	Security	
roup or user names:					
🔏 Vadim B. Ka (vbk	@diff.pki)			^	
As-1-5-21-947200	811-1917850035	-2235440	96-16005		
🥈 admin (admin@di	ff.pki)			=	
👗 Администратор	Информ Безопа	всности	(aib@diff.pki)		
CertIssuers (DIFF	CertIssuers)				
Test Aib (testaib)	ediff.pki)				
ServiceCA4 (servi	CECA4@dill.pki/	520. 20.		~	
		Δ	44	Domaura	
			DO	nemove	
	202			Nemove	
ermissions for CertIss	uers		Allow	Deny	
ermissions for CertIss Read	uers		Allow	Deny	
ermissions for CertIss Read Issue and Manage (uers Certificates		Allow	Deny	
ermissions for CertIss Read Issue and Manage (Manage CA	uers Certificates		Allow		
ermissions for CertIss Read Issue and Manage (Manage CA Request Certificates	uers Certificates		Allow		
ermissions for CertIss Read Issue and Manage (Manage CA Request Certificates	uers Certificates		Allow		
ermissions for CertIss Read Issue and Manage (Manage CA Request Certificates	uers Certificates		Allow		
ermissions for CertIss Read Issue and Manage (Manage CA Request Certificates	uers Certificates		Allow		
ermissions for CertIss Read Issue and Manage (Manage CA Request Certificates	uers Certificates		Allow		
ermissions for CertIss Read Issue and Manage (Manage CA Request Certificates	uers Certificates		Allow		

Рисунок 3.8 – Добавление разрешений для группы издателей сертификатов

Установите для группы разрешение **Выпуск и управление сертификатами (Issue** and Manage Certificates) и Запросить сертификаты (Request Certificates) и нажмите OK (рисунок 3.8).

В левой части окна перейдите на пункт **Шаблоны сертификатов (Certificate Templates)**, щелкните правой кнопкой мыши и выберите **Управление (Manage)** (рисунок 3.9).



al .			certsry - [0	Certification Authority (Local)\diff-S18CA02-CA\Certificate Templates]	_ 0
File Action View H	elp				
	2				
Certification Authority	(Local)	Name	•	Intended Dumore	
A J diff-S18CA02-CA	iff-S18CA02-CA Revoked Certificates Issued Certificates			Minned Topose	
Revoked Certific			ator	Encode and a second and a secon	
Issued Certificat				Client Authentication Secure Authentic	
Pending Reque	sts	Copy of Enrollment Agent		Cartificate Result Asset	
Failed Requests				Certificate Request Agent	
Certificate Tem		all Directory Email Replication		Client Authentication Secure Authentic	
	Mar	Manage troller Authentication New y Agent View boent		Client Authentication, Server Authentic	
	Nev			Citeric Addrenication, Server Addrenicc	
	View			Catificate Request Apart	
	VIEV	Refresh Agent Different Export List thentication Help thentication with ViPNet		Certificate Request Agent	
	Refr			Smart Card Logon Client Authenticatio	
	Expe			Client Authentication Server Authentic	
	Hels			KDC Authentication, Smart Card Longon	
1	10000	One Day	Smartcard Lonon RSA	Client Authentication Smart Card Lonon	
		PKI Com	uter	Server Authentication, Client Authentic	
		PKI Enroll	ment Agent (Computer)	Certificate Request Agent	
		PKI Smart	card User (EA)	Smart Card Logon, Client Authenticatio	
		PKI Web S	Server	Server Authentication	
		Smartcard	Logon RSA	Smart Card Logon, Client Authentication	
		Smartcare	Logon RSA 2	Client Authentication Smart Card Logon	
		Smartcard Logon RSA 234		Smart Card Logon, Client Authentication	
		Smartcard	Logon ViPNet	Smart Card Logon, Client Authentication	
		Subordina	ate Certification Authority	<all></all>	
		🖳 User		Encrypting File System, Secure Email, Cl.,	
		Web Serve	er	Server Authentication	

Рисунок 3.9 – Управление шаблонами сертификатов

В появившемся окне выберите пункт *Агент регистрации (Enrollment Agent)* (рисунок 3.10).

Настройка свойств шаблона сертификата может осуществляться в уже имеющемся шаблоне, либо в созданной копии имеющегося шаблона.

Для создания копии имеющегося шаблона, щелкните правой кнопкой мыши и выберите *Скопировать шаблон (Duplicate Template)* (рисунок 3.10).

₽.	Certificate	Templates Console		_ _ X
File Action View Help				
(+ +) 🗊 🗟 🖬 🖬				
Certificate Templates (s18DC02.diff.pki)	Template Display Name	Schema Version	Versi	Intended Purposes
	R Code Signing	1	3.1	
	@ Computer	1	5.1	
	Representation of Smartcard Logon RSA	2	100.66	Client Authentication, Smart Card Logon
	Copy of Enrollment Agent	2	100.8	Certificate Request Agent
	Cross Certification Authority	2	105.0	
	Directory Email Replication	2	115.0	Directory Service Email Replication
	R Domain Controller	1	4.1	
	Domain Controller Authentication	2	110.0	Client Authentication, Server Authentication, Sma
	EFS Recovery Agent	1	6.1	
	Enrollmer		4.1	
	B Enrollmer Duplicate Template		5.1	-
	R Enrollmer All Tasks	•	102.2	Certificate Request Agent
	Exchange Properties		4.1	
	@ Exchange		6.1	
	R Exchange Help		7.1	
	@ IPSec	1	8.1	
	IPSec (Offline request)	1	7.1	
	JMS operator	2	100.3	Smart Card Logon, Client Authentication, Secure
	IMS operator true	2	100.3	Smart Card Logon, Client Authentication, Secure
	Kerberos Authentication	2	110.0	Client Authentication, Server Authentication, Sma
	Rerberos Authentication with ViPN	et 2	100.4	KDC Authentication, Smart Card Logon, Server Au
	Rey Recovery Agent	2	105.0	Key Recovery Agent
	OCSP Response Signing	3	101.0	OCSP Signing
	One Day Smartcard Logon RSA	2	100.55	Client Authentication, Smart Card Logon
	PKI Computer	2	100.3	Server Authentication, Client Authentication
	PKI Enrollment Agent (Computer)	2	100.6	Certificate Request Agent
	PKI Smartcard User (EA)	2	100.9	Smart Card Logon, Client Authentication, Secure
	RKI Web Server	2	100.3	Server Authentication
	RAS and IAS Server	2	101.0	Client Authentication. Server Authentication
	<			Activate Windows
Using this template as a base, creates a template	that supports Windows Server 2003 Enterp	rise CAs		Go to System in Control Pa

Рисунок 3.10 – Создание копии шаблона

В появившемся окне со свойствами шаблона выполните следующие настройки:

1) Введите имя создаваемого шаблона на вкладке **Общие (General)**. При необходимости настройте **Срок действия сертификата (Validity period)** и **Период обновления (Renewal period)** (рисунок 3.11).

Supersede Compatibility Template displ Enrollment Age Template name Enrollment Age	d Templa General ay name ent Toke e: ent Token	n System	Exte Handling	ensions Cryptography	Security Key Attestation
Compatibility C Template displ Enrollment Ag Template name Enrollment Age	General ay name ent Toke e: e: entToken	Request in System	Handling	Cryptography	Key Attestation
Template displ Enrollment Ag Template name EnrollmentAge	ayname: ent Toke e: entToken	n System			
Enrollment Ag Template name EnrollmentAge	ent Toke e: entToken	n System System			
Template name EnrollmentAge	e: entToken	System			
Validity period: 2 years Publish cert Do not a Director	tificate in automatic y	Active Di	Renewa 6 rectory oll if a dupli	al period: weeks	xists in Active

Рисунок 3.11 – Свойства шаблона, вкладка General

2) Во вкладке **Безопасность (Security)** добавьте сервисную учетную запись, от имени которой будет запрашиваться выпуск сертификатов для пользователей. Для этого нажмите кнопку **Добавить (Add)** и в появившемся окне найдите созданную учетную запись (в примере, **serviceCA**) (рисунок 3.12 а, б).



Proj	perties	of New	Template	×			
Subject Name	Sen	/er	Issuance	Requirements			
Compatibility General	Request	Handling	Cryptography	Kev Attestation			
Superseded Templa	tes	Exte	ensions	Security			
Group or user names: Authenticated Users CertIssuers (DIFF\CertIssuers) ServiceCA (serviceCA@diff.pki) admin adminoff (Administrator) Domain Admins (DIFF\Domain Admins) Enterprise Admins (DIFF\Enterprise Admins)							
Permissions for service(CA		Add	Remove			
Full Control							
Read			✓				
Write							
Enroll							
Autoenroll							
For special permissions or advanced settings, click Advanced Advanced.							
ОК		Cancel	Act Apply t	Wate Wind System in C			
		a)					

Select this object type:	
Users, Groups, or Built-in security principals	Object Types
From this location:	
diff.pki	Locations
Enter the object names to select (examples):	
serviceCA (serviceCA@dlff.pki)	Check Names

б)

Рисунок 3.12 – Свойства шаблона, вкладка Security

3) Установите для сервисной учетной записи разрешение **Заявка (Enroll)** (рисунок 3.13).



Properties of New Template								
Subject N	lame	Ser	ver	Issuance R	equirements			
Compatibility	General	Request	Handling	Key Attestation				
Supersec	ded Templa	tes	Exte	ensions	Security			
Group or use	Group or user names:							
& dl_Enro & g_Etok & admin a & Domain & Enterpri	Image: ServiceCA (serviceCA (servic							
<			111		>			
Permissions Full Contro Read Write	Add Remove Permissions for serviceCA Allow Deny Full Control							
vvrite								
[ОК		Cancel	Apply	Help			

Рисунок 3.13 – Добавление разрешений для сервисной учетной записи

4) Во вкладке *Имя субъекта (Subject Name)* установите параметр *Строится на* основе данных Active Directory (Build from this Active Directory information) и нажмите *Применить (Apply)* (рисунок 3.14).



Compatibility General	Request	Handling	Cryptography	Key Attestation
Superseded Temp	ates	Exte	ensions	Security
Subject Name	Sen	ver	Issuance Re	equirements
Use subject inf renewal reques	est ormation fro sts (*)	m existing	certificates for a	utoenrollment
Select this option to simplify certificate a Subject name formation	enforce co dministration at:	nsistency 1.	among subject n	ames and to
Fully distinguished	name			~
Include e-mail n Include this informa E-mail name DNS name	ame in subje tion in altern	ect name nate subjec	t name:	
Service principa	I name (SPI	N)		
* Control is disabled du	ue to <u>compa</u>	atibility setti	ings.	

Рисунок 3.14 – Установка параметра *Строится на основе данных Active Directory*

5) Для сохранения шаблона нажмите **ОК**.

6) Для публикации созданного шаблона, после его настройки, перейдите на пункт Шаблоны сертификатов (Certificate Templates), щелкните правой кнопкой мыши и выберите Создать (New) → Выдаваемый шаблон сертификата (Certificate Template to Issue) (рисунок 3.15).

i	certsrv - [Certi	ficatio	n Authority (Local)\diff-S18C	A02-C/	A\Certificate Templates]	D X
File Action Vie	w Help					
🧢 🔿 🙎 🧟	🗟 【					P.
違 Certification Au	thority (Local)	Name		Intende	ed Purpose	^
⊿ 👼 diff-S18CA0	2-CA	🖳 CA	Exchange	Private	Key Archival	
📔 Revoked	Certificates	🗷 Sm	artcard Logon RSA 3	Client Authentication, Smart Card Logon		
Issued Co	ertificates	🗷 Sm	artcard Logon RSA 234	Smart	Card Logon, Client Authentication	
Pending	Requests	🗷 Sm	artcard Logon RSA 2	Client	Authentication, Smart Card Logon	
Failed Re	quests	🗷 JM	S operator true	Smart	Card Logon, Client Authenticatio	
Certificat	Manage		Day Smartcard Logon RSA	Client	Authentication, Smart Card Logon	
_	Manage		Allment Agent	Certific	ate Request Agent	
	New	•	Certificate Template to Issue		ite Request Agent	=
	View	+	Computer	Server	Authentication, Client Authentic	
	Defeat		Web Server	Server	Authentication	
	Kerresn		Smartcard User (EA)	Smart	Card Logon, Client Authenticatio	
	Export List		Ilment Agent 4 Different	Certific	ate Request Agent	
	Help		irtcard Logon ViPNet		Card Logon, Client Authentication	
		🛎 Sm	artcard Logon RSA	Smart Card Logon, Client Authentication		
		🖳 Ke	beros Authentication with ViPNet	KDC Authentication, Smart Card Logon		
		🗷 Dir	ectory Email Replication	Directory Service Email Replication		
		🗷 Do	main Controller Authentication	Client Authentication, Server Authentic		
		🖳 Ke	beros Authentication	Client Authentication, Server Authentic		
		🖳 EFS	Recovery Agent	File Re	covery	
		🚇 Bas	sic EFS	Encryp	ting File System	
		🗷 Do	main Controller	Client	Authentication, Server Authentic	~
Enable additional Ce	rtificate Template	s on this	Certification Authority			

Рисунок 3.15 – Выбор выдаваемого шаблона сертификата

7) В появившемся окне (рисунок 3.16) выберите созданный шаблон сертификата и нажмите **ОК**.

Enable Certificate Templates							
Select one Certificate Template to enable on this O Note: If a certificate template that was recently cre information about this template has been replicated All of the certificate templates in the organization m For more information, see <u>Certificate Templa</u>	Certification Authority. Hated does not appear on this list, you may need to wait until d to all domain controllers. Hay not be available to your CA. Hate Concepts.						
Name	Intended Purpose	~					
R Authenticated Session	Client Authentication						
Reference CEP Encryption	Certificate Request Agent	_					
🚇 Code Signing	Code Signing	=					
🚇 Copy 2 of Smartcard Logon RSA	Client Authentication, Smart Card Logon						
Reprint Encollment Agent	Certificate Request Agent						
Cross Certification Authority	<al></al>						
Enrollment Agent (Computer)	Certificate Request Agent						
🚇 Enrollment Agent Token System	Certificate Request Agent						
Representation of the second s	Certificate Request Agent						
Exchange Signature Only	Secure Email						
R Exchange User	Secure Email	\sim					
	OK Cance	4					



3.2 Сертификат пользователя

При выпуске токена с сертификатом, в память токена записывается сертификат, выпущенный по шаблону сертификата пользователя со смарт-картой. Данный

сертификат, позволяет осуществлять пользователю вход в систему.

Для создания шаблона запустите консоль центра сертификации с помощью команды *certsrv.msc* в командной строке (рисунок 3.17).





Окно консоли будет выглядеть следующим образом:

📮 certs	rv - [Certification Authority (Local)\	diff-S18CA02-CA\Certificate Templa	ites]
File Action View Help			
🗢 🔿 🙍 🧟 👔			
 Certification Authority (Local) diff-S18CA02-CA Revoked Certificates Issued Certificates Pending Requests Failed Requests Certificate Templates 	Name Enrollment Agent Default Smartcard Logon RSA 3 Smartcard Logon RSA period Smartcard Logon RSA 1 Day Smartcard Logon RSA 1 Day Smartcard Logon RSA 5 Days Smartcard Logon RSA 15 Days Smartcard Logon RSA 1 Year Smartcard Logon RSA 0 ne Month CA Exchange Smartcard Logon RSA 2 JMS operator true One Day Smartcard Logon RSA Enrollment Agent PKI Enrollment Agent (Computer) PKI Computer PKI Smartcard User (EA) Enrollment Agent 4 Different	Intended Purpose Certificate Request Agent Client Authentication, Smart Card Logon Client Authentication, Smart Card Logon Smart Card Logon, Client Authentication Client Authentication, Smart Card Logon Smart Card Logon, Client Authenticatio Client Authentication, Smart Card Logon Certificate Request Agent Server Authentication, Client Authentic Server Authentication Smart Card Logon, Client Authentic Server Authentication Smart Card Logon, Client Authenticatio Certificate Request Agent	
	Smartcard Logon ViPNet	Smart Card Logon, Client Authentication Smart Card Logon, Client Authentication	
	Rerberos Authentication with ViPNet	KDC Authentication, Smart Card Logon	

Рисунок 3.18 – Консоль центра сертификации

В левой части окна перейдите на пункт *Шаблоны сертификатов (Certificate Templates)*, щелкните правой кнопкой мыши и выберите *Управление (Manage)* (рисунок 3.19).

i	certs	rv - [Cert	tification Authority (Local)\	diff-S18CA02-CA\Certificate Templa	ates] 🗕 🗖 🗙	
File Action View	Help					
← ⇒ 2 0 ≥	?					
🙀 Certification Authori	rity (Local)	Name		Intended Purpose		~
a 🚽 diff-S18CA02-CA	4	🗷 Enrol	lment Agent Default	Certificate Request Agent		
Revoked Cert	tificates	🗷 Smar	tcard Logon RSA 3	Client Authentication, Smart Card Logon		
📔 Issued Certifi	icates	🚇 Smar	tcard Logon RSA period	Client Authentication, Smart Card Logon		
Pending Requ	uests	🗷 Smar	tcard Logon RSA 1 Day	Client Authentication, Smart Card Logon		
Failed Reques	ests	🗷 Smar	tcard Logon RSA 5 Days	Client Authentication, Smart Card Logon		
Certificat-	Manage		card Logon RSA 15 Days	Client Authentication, Smart Card Logon		
			card Logon RSA 1 Year	Client Authentication, Smart Card Logon		
	New	•	card Logon RSA One Month	Client Authentication, Smart Card Logon		
	View	•	change	Private Key Archival		
	Refresh	card Logon RSA 234		Smart Card Logon, Client Authentication	1	=
	EvenetList		card Logon RSA 2	Client Authentication, Smart Card Logon		
	Export List.		perator true	Smart Card Logon, Client Authenticatio		
	Help		ay Smartcard Logon RSA	Client Authentication, Smart Card Logon		
		🚇 Enrol	Iment Agent	Certificate Request Agent		
		🚇 PKI E	nrollment Agent (Computer)	Certificate Request Agent		
		🚇 PKI C	omputer	Server Authentication, Client Authentic		
		🚇 PKI V	/eb Server	Server Authentication		
		🚇 PKI S	martcard User (EA)	Smart Card Logon, Client Authenticatio		
		🚇 Enrollment Agent 4 Different		Certificate Request Agent	-	-
		🚇 Smar	tcard Logon ViPNet	Smart Card Logon, Client Authentication		
		🚇 Smar	tcard Logon RSA	Smart Card Logon, Client Authentication		
		🚇 Kerbe	eros Authentication with ViPNet	KDC Authentication, Smart Card Logon		
		🚇 Direc	tory Email Replication	Directory Service Email Replication		
		🖳 🖳 Dom	ain Controller Authentication	Client Authentication, Server Authentic		
		🖳 Kerbe	eros Authentication	Client Authentication, Server Authentic		

Рисунок 3.19 – Управление шаблонами сертификатов

В появившемся окне выберите пункт **Пользователь со смарт-картой (Smartcard** *Logon)*, щелкните правой кнопкой мыши и выберите **Скопировать шаблон (Duplicate** *Template)* (рисунок 3.20).

Certificate Templates Console						
File Action View Help						
🗢 🔿 🔲 🖴 📔 🖬						
Rertificate Templates (s18DC02.diff.pki)	Template Display Name		Schema Versior	n Version	Intended Purposes ^	
	JMS operator true		2	100.3	Smart Card Logon, Client Authe	
	Kerberos Authentication		2	110.0	Client Authentication, Server Au	
	🚇 Kerberos Authentication with \	/iPNet	2	100.4	KDC Authentication, Smart Care	
	🚇 Key Recovery Agent	🗷 Key Recovery Agent 2			Key Recovery Agent	
	OCSP Response Signing		101.0	OCSP Signing		
	🚇 One Day Smartcard Logon RSA	4	2	100.55	Client Authentication, Smart Ca	
	PKI Computer		2	100.3	Server Authentication, Client Au	
	🚇 PKI Enrollment Agent (Compu	ter)	2	100.6	Certificate Request Agent	
	PKI Smartcard User (EA)		2	100.9	Smart Card Logon, Client Authe	
	🚇 PKI Web Server		2	100.3	Server Authentication	
	RAS and IAS Server		2	101.0	Client Authentication, Server Au	
	Root Certification Authority		1	5.1		
	Router (Offline request)		1	4.1		
	🚇 Smartcard Logon		1	6.1		
	Smartcard Logon Default	Duplicate Template		100.2	Smart Card Logon, Client Authe	
	Real Smartcard Logon RSA	All Tasks	•	100.112	Smart Card Logon, Client Authe	
	🚇 Smartcard Logon RSA 1 D			100.102	Client Authentication, Smart Ca _	
	Smartcard Logon RSA 1 Y	Properties		100.103	Client Authentication, Smart Ca	
	Real Smartcard Logon RSA 15	Help		100.101	Client Authentication, Smart Ca	
	🚇 Smartcard Logon RSA 2		2	100.223	Client Authentication, Smart Ca	
	🚇 Smartcard Logon RSA 234		2	100.80	Smart Card Logon, Client Authe	
	🚇 Smartcard Logon RSA 3		2	100.284	Client Authentication, Smart Ca	
	🚇 Smartcard Logon RSA 5 Days		2	100.101	Client Authentication, Smart Ca	
	🚇 Smartcard Logon RSA One Mo	nth	2	100.103	Client Authentication, Smart Ca	
	🚇 Smartcard Logon RSA period		2	100.120	Client Authentication, Smart Ca	
	Smartcard Logon ViPNet		2	100.6	Smart Card Logon, Client Authe	
	Smartcard User		1	11.1	×	
	<	Ш		2	>	

Рисунок 3.20 -	Создание	копии	шаблона
----------------	----------	-------	---------

В появившемся окне со свойствами шаблона выполните следующие настройки:

1) Введите имя создаваемого шаблона на вкладке *Общие (General)* (рисунок 3.21).

Prop	perties	of New	Template	x			
Subject Name	Sen	ver	Issuance R	equirements			
Superseded Templa	tes	Exte	nsions	Security			
Compatibility General	Request	Handling	Cryptography	Key Attestation			
Template display name:							
Smartcard Logon RSA							
Template name: SmartcardLogonRSA Validity period: 1 years ✓	Template name: SmartcardLogonRSA Validity period: Renewal period:						
Validity period: 1 years 6 weeks v Publish certificate in Active Directory Do not automatically reenroll if a duplicate certificate exists in Active Directory Directory Directory							
ОК	(Cancel	Apply	Help			

Рисунок 3.21 – Свойства шаблона, вкладка General

2) Во вкладке **Безопасность (Security)** добавьте сервисную учетную запись, от имени которой будет запрашиваться выпуск сертификатов для пользователей. Для этого нажмите кнопку **Добавить (Add)** и в появившемся окне найдите созданную учетную запись (в примере, **serviceCA**) (рисунок 3.22 а, б).



Pro	perties of Ne	ew Template	x				
Subject Name	Server	Issuance R	equirements				
Compatibility General	Request Handli	ng Cryptography	Key Attestation				
Superseded Templa	stes	Extensions	Security				
Group or user names:							
Authenticated Users							
& g_Enrolment_Age	nt (DIFF\g_Enrol	ment_Agent)					
& dl_Enrolment_Age	nt (DIFF\dl_Enro	lment_Agent)					
🦓 g_Etoken.Admin (I	DIFF\g_EtokenAc	dmin)					
👗 admin adminoff (A	dministrator)						
Domain Admins (L	(DIEE) Entermine	nins) Admine)					
Chiterprise Adminis	(DIFF \Enterprise	Admins)					
		LLA .	Demons				
		Add	Remove				
Permissions for Authent	ticated Users	Allow	Deny				
Full Control							
Read		✓					
Write							
Enroll							
Autoenroll							
For special permissions	or advanced set	tings, click	Advanced				
Advanced.			1.0.0				
ОК	Cancel	Apply	Help				

a)

Select this object type:	
Users, Groups, or Built-in security principals	Object Types
From this location:	
diff.pki	Locations
Enter the object names to select (<u>examples</u>): serviceCA (serviceCA@dfff_pki)	Check Names
Enter the object names to select (<u>examples</u>): serviceCA (serviceCA@diff.pki)	Check Names
Enter the object names to select (<u>examples</u>): serviceCA (serviceCA@diff.pki)]	Check Names

б)

Рисунок 3.22 – Свойства шаблона, вкладка Security

3) Установите для сервисной учетной записи разрешение **Заявка (Enroll)** (рисунок 3.23).



Properties of New Template							
Subject N	lame	Ser	ver	Issuance R	equirements		
Compatibility	General	Request	Handling	Cryptography	Key Attestation		
Supersec	Superseded Templates Extensions Security						
Group or user names:							
& dl_Enro & g_Etok & admin a & Domain & Enterpri	Image: ServiceCA (serviceCA(@diff.pki))						
<					>		
Permissions	for service(CA	[Add Allow	Remove Deny		
Full Contro	d						
Read							
Write							
Enroll				✓			
Autoenroll							
[ОК		Cancel	Apply	Help		

Рисунок 3.23 – Добавление разрешений для сервисной учетной записи

4) Для выпуска сертификата средствами подсистемы управления жизненным циклом токенов, в окне со свойствами шаблона перейдите во вкладку *Имя субъекта (Subject Name)* и установите переключатель на параметр *Предоставляется в запросе (Supply in the request)* (рисунок 3.24).



Properties of New Template							
Superseded Templa	Superseded Templates Extensions Security						
Compatibility General	Request	Handling	Cryptography	Key Attestation			
Subject Name	Sen	ver	Issuance F	Requirements			
 Supply in the request Use subject information from existing certificates for autoenrollment renewal requests (*) 							
 Build from this Active Select this option to e simplify certificate adm 	Directory Inforce co ninistration	nsistency	n among subject r	names and to			
Subject name format:							
None				×			
Include e-mail nam	ne in subje	ect name					
Include this information	Include this information in alternate subject name: E-mail name DNS name User principal name (UPN) Service principal name (SPN)						
* Control is disabled due	to compa	atibility sett	Apply	Help			

Рисунок 3.24 – Настройка выпуска сертификата пользователя средствами подсистемы

5) Во вкладке *Шифрование (Cryptography)* установите минимальный размер ключа шифрования – 1024 бит (рисунок 3.25).



Prop	Properties of New Template								
Subject Name	Server	Issuance R	equirements						
Superseded Templa	tes E	tensions	Security						
Compatibility General	Request Handling	Cryptography	Key Attestation						
Provider Category:	Provider Category: Legacy Cryptographic Service Provider V								
Algonium name.	Algorithm hame: Determined by CSP								
Minimum key size:	1024								
Choose which cryptogra Requests can use a Requests must use a Providers: Athena ASECard Cry Te Token Base Crypto Infotecs GOST 2012 Microsoft Base DSS	Choose which cryptographic providers can be used for requests Requests can use any provider available on the subject's computer Requests must use one of the following providers: Providers: Athena ASECard Crypto CSP e Token Base Cryptographic Provider Infotecs GOST 2012/1024 Cryptographic Service Provider Microsoft Base Cryptographic Provider v1.0 Microsoft Base DSS and Diffie-Hellman Cryptographic Provide Y 								
Request hash:	Determined t	y CSP	~						
Betermined by CSP									
ОК	Cancel	Apply	Help						

Рисунок 3.25 – Установка минимального размера ключа шифрования

6) Для сохранения шаблона нажмите **ОК**.

Для публикации созданного шаблона, после его настройки, перейдите на пункт *Шаблоны сертификатов (Certificate Templates)*, щелкните правой кнопкой мыши и выберите *Создать (New)* → *Выдаваемый шаблон сертификата (Certificate Template to Issue)* (рисунок 3.26).

i	certsrv - [Certi	ficatio	n Authority (Local)\diff-S18C	A02-C	A\Certificate Templates]	×
File Action V	iew Help					
🧇 🔿 🖄 🤷	🔒 🔽					
違 Certification A	uthority (Local)	Name		Intend	ed Purpose	^
⊿ 🚽 diff-S18CA	02-CA	CA Exchange		Private	Key Archival	
Revoked Certificates		Real Smartcard Logon RSA 3		Client Authentication, Smart Card Logon		
📔 Issued (Certificates	🖳 Sm	artcard Logon RSA 234	Smart	Card Logon, Client Authentication	
Pending	g Requests	🗷 Sm	artcard Logon RSA 2	Client	Authentication, Smart Card Logon	
Failed R	lequests	🖳 JM	S operator true	Smart	Card Logon, Client Authenticatio	
Certific	Manage		Day Smartcard Logon RSA	Client	Authentication, Smart Card Logon	
	wanage		Allment Agent	Certific	ate Request Agent	
	New	•	Certificate Template to Issue		ite Request Agent	=
	View	+	Computer	Server	Authentication, Client Authentic	
	Defeash		Web Server	Server	Authentication	
	Keiresh		Smartcard User (EA)	Smart	Card Logon, Client Authenticatio	
	Export List		Ilment Agent 4 Different	Certific	ate Request Agent	
	Help		irtcard Logon ViPNet		Card Logon, Client Authentication	
		🛎 Sm	artcard Logon RSA	Smart	Card Logon, Client Authentication	
		🖳 Ke	beros Authentication with ViPNet	KDC A	uthentication, Smart Card Logon	
		🚇 Dir	ectory Email Replication	Directo	ory Service Email Replication	
		🖳 Do	main Controller Authentication	Client	Authentication, Server Authentic	
		🖳 Ke	beros Authentication	Client Authentication, Server Authentic		
		🖳 EFS	Recovery Agent	File Recovery		
		🚇 Bas	sic EFS	Encryp	ting File System	
		🖳 Do	main Controller	Client	Authentication, Server Authentic	~
Enable additional C	ertificate Template	s on this	Certification Authority			

Рисунок 3.26 – Выбор выдаваемого шаблона сертификата

В появившемся окне (рисунок 3.27) выберите созданный шаблон сертификата и нажмите **ОК**.

Enable C	Certificate Templates	x
Select one Certificate Template to enable on this 0 Note: If a certificate template that was recently cre nformation about this template has been replicater All of the certificate templates in the organization m For more information, see <u>Certificate Templa</u>	Certification Authority. Pated does not appear on this list, you may need to wait until d to all domain controllers. Nay not be available to your CA. <u>Ste Concepts.</u>	
Name	Intended Purpose	~
R Authenticated Session	Client Authentication	
CEP Encryption	Certificate Request Agent	
🗷 Code Signing	Code Signing	=
🚇 Smartcard Logon RSA	Client Authentication, Smart Card Logon	
Reprint Agent Copy of Enrollment Agent	Certificate Request Agent	
Cross Certification Authority	<al></al>	
Enrollment Agent (Computer)	Certificate Request Agent	
🗷 Enrollment Agent Token System	Certificate Request Agent	
Representation of the second s	Certificate Request Agent	
Exchange Signature Only	Secure Email	
R Exchange User	Secure Email	~
	OK Canc	el

Рисунок 3.27 – Публикация созданного шаблона

4 Настройки на сервере «Блокхост-Сеть»

4.1 Выпуск и установка сертификата агента регистрации

Выпуск и установка сертификата агента регистрации осуществляется на рабочее место администратора безопасности с установленной серверной версией средства защиты от несанкционированного доступа «Блокхост-Сеть 4».

Для возможности выпуска сертификатов пользователей, необходимо наличие в оснастке **Сертификаты (Certificates)** в разделе **Личные (Personal)** установленного сертификата, выпущенного по шаблону сертификата агента регистрации.

Для создания сертификата выполните следующие действия:

1) Выполните вход в систему под сервисной учетной записью (*serviceCA*) и перейдите в оснастку сертификатов *certmgr.msc*, либо выполните вход в систему под административной учетной записью и запустите оснастку сертификатов (рисунок 4.1) изпод сервисной учетной записи командой

🚋 certmgr - [Сертификаты - текущий пользователь] 🚡 Файл Действие Вид Избранное Окно Справка - 8 × 🦛 🔿 🔚 🖸 📰 🗊 Сертификаты - текущий пользователь Имя логического хранилища 🧮 Личное 🚞 Личное Доверенные корневые центры сертификации 🚞 Доверенные корневые центры сертификации Доверительные отношения в предприятии Доверительные отношения в предприятии Промежуточные центры сертификации 📔 Промежуточные центры сертификации Объект пользователя Active Directory 📔 Объект пользователя Active Directory Доверенные издатели Доверенные издатели Сертификаты, к которым нет доверия 🚞 Сертификаты, к которым нет доверия Сторонние корневые центры сертификации 🚞 Сторонние корневые центры сертификации Доверенные лица 🚞 Доверенные лица Запросы заявок на сертификат 🗎 Запросы заявок на сертификат Доверенные корневые сертификаты смарт-карты 🛄 Доверенные корневые сертификаты смарт-карты

runas /user:<домен\имя пользователя> "cmd /C start /B certmgr.msc"

Рисунок 4.1 – Оснастка Сертификаты (Certificates)

2) В левой части окна перейдите в раздел *Личные (Personal)* и по щелчку правой кнопкой мыши выберите *Bce задачи (All Task)* → *Запросить новый сертификат (Request New Certificate)* (рисунок 4.2).



🚡 certmgr - [Сертификаты - текущий пользов	атель\Личное]			
🚰 Файл Действие Вид Избранное О	кно Справка		_ 8 ×	
🙀 Сертификаты - текущий пользователь		Тип объекта		
Пичное Поиск сертификатов	ации	🚞 Сертификаты		
Все задачи 🔸	Поиск се	ртификатов		
Вид +	Запроси	ъ новый сертификат		
Новое окно отсюда	Импорт.			
Новый вид панели задач	Дополни	1ополнительные операции		
 Обновить Экспортировать список 	рт-карты			
Справка				
	-			
 Запросить новый сертификат от центра сертиф	икации (ЦС) в	том домене		

Рисунок 4.2 – Запрос нового личного сертификата

3) В появившемся окне **Регистрация сертификатов** выберите **Политика** *регистрации Active Directory (Active Directory Enrollment Policy)* и нажмите **Далее** (рисунок 4.3).

Регистрация сертификатов	
Выбор политики регистрации сертификатов	
Политика регистрации сертификатов позволяет регистрировать заранее шаблонов сертификатов. Политика регистрации сертис	о сертификаты на основании заданных фикатов уже могла быть настроена.
Настраиваемые администратором	
Политика perистрации Active Directory	*
Настраиваемые пользователем	Добавить
Дополнительные сведения о <u>политике регистрации сертификат</u>	08

Рисунок 4.3 – Выбор политики регистрации сертификата

4) Выберите шаблон сертификата, созданный в центре сертификации (например,



Enrollment Agent Token System) (рисунок 4.4).

Регистрация сертификатов			
Запрос сертификатов Можно запросить следующие типы с запросить, а затем нажмите кнопку "З	ертификатов. Выберите сертификат Заявка".	ы, которые необходимо	
Active Directory Enrollment Policy			*
Enrollment Agent Token System	Остояние: Доступно	Подробности 💙	
One Day Smartcard Logon RSA Требуется больше данных для настройки параметров	Остояние: Доступно для подачи заявки на этот сертифика.	Подробности 💙 кат. Щелкните здесь	
Smartcard Logon RSA	Остояние: Доступно	Подробности 💙	
Требуется больше данных для настройки параметров	для подачи заявки на этот сертифи в.	кат. Щелкните здесь	+
Показать все шаблоны Дополнительные сведения о сертифи	катах		
		<u>З</u> аявка Отме	ена

Рисунок 4.4 – Выбор шаблона сертификата

5) Дождитесь выпуска и установки сертификата в хранилище **Личное** (рисунок 4.5 а) и нажмите **Готово** (рисунок 4.5 б).

📮 Pe	гистрация сертификатов		
	Результаты установки сертиф	икатов	
	Следующие сертификаты были получ Active Directory Enrollment Policy	ены и установлены на данном компь	ютере.
	☑ Enrollment Agent Token System	√ Состояние: Успешно	Подробности 🗸
			<u>Г</u> отово



Консоль1 - [Корень консоли\Сертификаты - текул	щий пользователь\Лично <u>С</u> правка	е\Сертификаты]						- # x
🗢 🔿 🖄 📰 🤞 🔀 🖸 🖬								
Корень консоли	Кому выдан	Кем выдан	Срок действия	Назначения	Имя	Сост Шаб	Действия	
 Сертификаты - текущии пользователь Пичное 	ServiceCA	diff-S18CA02+CA	30.06.2021	Агент запроса сер	<her></her>	Enro	Сертификаты	
🕮 Сертификаты							Дополнительные действия	•
 Доверенные корневые центры сертифик Зарадительные отколнение в посториях 							serviceCA5	-
 Промежуточные центры сертификации Объект пользователя Асбие Directory Доверенные адателя Сертификаты, которым нет доверна Сертификаты, которым нет доверна Доверенные плана Доверенные корнивецие сертификаты сина Доверенные корнивецие сертификаты сина 							Дополнительные действия	,
۰ <u>س</u> ،	4		211					
Хранилище Личное содержит 1 сертификат.								

б)

Рисунок 4.5 – Установка сертификата в хранилище Личное

4.2 Создание профилей в настройках подсистемы

Для корректной работы подсистемы управления жизненным циклом токенов по выпуску сертификатов необходимо создать профиль для выпуска сертификата в настройках подсистемы управления жизненным циклом токенов.

Откройте консоль администрирования Блокхост-Сеть и перейдите в раздел Настройки

→ **Выпуск сертификатов** по кнопке ^(©) (рисунок 4.6).

🔀 Блок	схост-Сеть 4					-		×
&	Настройки							
κ∱π	Выпуск сертификатов*	Выпуск сертификатов						
70	Другие параметры	🕙 Создать профиль 🔍 Поиск				Все типы	Ŧ	ו
8	Почтовые уведомления	💿 Просмотреть 🖉 Изменить	🗑 Удалить					
	Шаблоны актов	Профиль 🔻 Тип УЦ	Прокси-клиент Домен	Имя пользователя	Центр сертификаци	Шаблон сертифика	Описани	le
		Профиль 3 🚸 Microsoft CA	W102 pki.local	pki.local\serviceca	s09dc.pki.local\	SmartcardLogo		
		Профиль 2 🗳 Microsoft CA	pki.local	pki.local\service_user	s09dc.pki.local\	SmartcardLogo		
		Профиль1 🔶 Microsoft CA	pki.local	pki.local\serviceca	s09dc.pki.local\	SmartcardLogo		
E								
£2.	Применить Отмена							
8								

Рисунок 4.6 – Раздел Настройки

Для каждого созданного профиля в окне **Выпуск сертификатов** отображается информация:

- Профиль наименование профиля;
- Тип УЦ центр сертификации выпускающий сертификат (Microsoft CA/DogTag);

– *Прокси*-клиент – клиентская рабочая станция, выбранная для взаимодействия с центром сертификации;

- *Домен* наименование домена;
- Имя пользователя наименование сервисной учетной записи;
- Центр сертификации адрес центра сертификации;
- *Шаблон сертификата* шаблон сертификата для входа;
- Описание подробное описание профиля.

При необходимости, любой из созданных профилей возможно изменить или удалить с помощью соответствующих кнопок в верхней части вкладки (рисунок 4.6).

4.2.1 Создание профиля Microsoft CA

Для создания профиля по выпуску сертификатов центра сертификации Microsoft CA

G	S сервис	СЗИ от Руковод Настрой	НСД «Блокхост-Сеть 4» цство администратора безопа йка подсистемы управления т	сности. Часть 3 окенами, ЦС Microsoft CA
наж	мите на кнопку 💿	и выберите	<i>Microsoft CA</i> (рису	нок 4.7).
🗙 Бло	окхост-Сеть 4			- 🗆 ×
Å	Настройки			
к∱я	Выпуск сертификатов*	Выпуск сертификатов		
冏	Другие параметры	🕙 Создать профиль 🔍 Поиск		Все типы 💌
F	Почтовые уведомления	 FreeIPA/Dogtag Изменить ШУд Microsoft CA 	далить	
	Шаблоны актов	Прок	си-клиент Домен Имя пользователя	Центр сертификаци Шаблон сертифика ⁻ Описание
		Профиль 3 Ф Microsoft CA	W102 pki.local pki.local\serviceca	s09dc.pki.local\ SmartcardLogo

Рисунок 4.7 – Выбор центра сертификации

В появившемся окне (рисунок 4.8) введите наименование профиля, его описание, при необходимости, и параметры сервисной учетной записи (имя пользователя и пароль) в соответствующих полях.

🔀 Создание профиля Act	tive Directory	2
Имя профиля		
Профиль 4		
Описание		
Введите описание прос	филя	
Указать прокси-клиен	нт для предоставления д	оступа 🛈
Каталог учетных за	аписей 🛈	
Active Directory		
pki.local		
Выпуск сертифика	тов	
Имя пользователя 🛈	serviceca	
Пароль	•••••	O
	Подключиться	
	Создать	Отмена

Рисунок 4.8 – Создание профиля AD

Нажмите кнопку Подключиться (рисунок 4.8).



При возникновении ошибки при подключении убедитесь, что для вводимой сервисной учетной записи или для группы, в которую учетная запись входит,
правилами клиентской политики безопасности не установлен запрет на аутентификацию Windows (подробное описание приведено в документе «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 1. Управление политиками»).

После успешного подключения произойдет запуск получения списка сертификатов выбранной сервисной учетной записи и в нижней части окна появится информация о подключении (рисунок 4.9).

🔀 Создание профиля Active Directory Имя профиля	×
Профиль 4]
Описание	
Введите описание профиля	
Указать прокси-клиент для предоставления доступа ③	J
Каталог учетных записей 😳	
Active Directory	
pki.local	
Выпуск сертификатов	
Имя пользователя 🛈 serviceca	
Пароль	
Изменить]
Имя центра сертификации Microsoft CA s09dc.pki.local\pki-S09DC-CA	
Сертификат агента регистрации - Enrollment Agent 🛈 C	.
46fcbcb7ebb9525ff819566a343ceb9c53623d02	1
Шаблон сертификата для входа С	
Не задано 🔹	
Таймаут ожидания при выпуске сертификата, сек 30]
Размер ключа, бит 1024 🚆]
Публиковать выдаваемые сертификаты в ActiveDirectory 🛈	
Создать Отмена	

Рисунок 4.9 – Выбор сертификата агента регистрации и шаблона для входа

В поле *Сертификат агента регистрации – Enrollment Agent* отобразится необходимый сертификат агента регистрации, установленный в личное хранилище оснастки *Сертификаты*.

 \bigcirc

Если в личном хранилище выбранной учетной записи несколько сертификатов, в поле *Сертификат агента регистрации – Enrollment Agent* появится возможность выбора необходимого сертификата по кнопке **Выбрать** *сертификат* (рисунок 4.10 а).

🗙 Создание профиля Active Directory	×
Имя профиля	
Профиль 4	
Описание	
Указать прокси-клиент для предоставления доступа 🛈	
Каталог учетных записей 🛈	
Active Directory	
pki.local	
Выпуск сертификатов	
Имя пользователя ③ serviceca	
Пароль	
Изменить]
Имя центра сертификации Microsoft CA	
s09dc.pki.local\pki-S09DC-CA	
Сертификат агента регистрации - Enrollment Agent 🛈 C	
Выбрать сертификат	
Создать Отмена	

a)



🗙 Выбор сертификата агента	арегистрации			×
Наименование	Издатель	Действителен от	Действителен до	
serviceca	pki-S09DC-CA	06.06.2023 16:39	05.06.2025 16:39	Ο
serviceca	pki-S09DC-CA	06.06.2023 16:30	05.06.2025 16:30	0
		Отмена	Применит	Ъ

б)

Рисунок 4.10 – Выбор сертификата агента регистрации из списка

При отсутствии в личном хранилище оснастки **Сертификаты** сертификата агента регистрации выбранной учетной записи, после попытки получения списка сертификатов, в окне настроек появится запись об отсутствии сертификата агента регистрации (рисунок 4.11).

Необходимо установить сертификат в личное хранилище, последовательно выполняя действия, описанные в разделе *Установка сертификата агента регистрации в хранилище,* и нажать кнопку ^С.

Имя центра сертификации Microsoft CA s09dc.pki.local\pki-S09DC-CA Сертификат агента регистрации - Enrollment Agent ③ С Отсутствует ④

Рисунок 4.11 – Отсутствие сертификата агента регистрации

После добавления сервисной учетной записи нажмите кнопку *Применить* для перезапуска службы *GIS.ServerTokenSystem*.

В поле *Шаблон сертификата для входа* (рисунок 4.12) необходимо выбрать из списка шаблон сертификата пользователя, созданный в центре регистрации (например, *SmartcardLogonCA*).

39



шавлоп сертификата для входа о
SmartcardLogonTokensystem
EFSRecovery
EnrollmentAgentCA
EnrollmentAgenttokensystem
KerberosAuthentication
Machine
SmartcardLogonCA

Рисунок 4.12 – Выбор шаблона сертификата для входа

Имя шаблона сертификата пользователя в поле Шаблон сертификата для входа соответствует имени, заданному при создании шаблона в центре сертификации на вкладке Общие (General) в параметре Имя шаблона (Template name) (рисунок 4.13).

Smartcard Logon RSA 2 Properties	? X
Subject Name Issuance Requirement	s
Superseded Templates Extensions Security	Server
General Compatibility Request Handling Cryptography Key	Attestation
Template display name:	
Smartcard Logon RSA 2	
Template name: SmartcardLogonRSA2	
Validity period: Validity per	
 Publish certificate in Active Directory Do not automatically reenroll if a duplicate certificate exists in Directory 	n Active
OK Cancel Apply	Help

Рисунок 4.13 – Шаблон сертификата для входа

После нажатия кнопки Создать профиль отобразится в списке и будет доступен к



выбору при выпуске токена пользователю для входа по сертификату (рисунок 4.14).

🗙 Выпуск токена для в	хода по управляемому сертификату	×
ruToken, S/N 0951209	993	
Пользователь	Иванов Иван Иванович 🖉 🔟	
Домен	♠ Active Directory	
Профиль выпуска	Профиль 1 🔹 💿	
Имя токена	Rutoken ECP <no label=""></no>	
Инвентарный номер		
Комментарий		
🔵 Инициализирова	ать Отмена Примени	ИТЬ

Рисунок 4.14 – Отображение профиля при выпуске токена

4.2.2 Добавление прокси-клиента для взаимодействия с ЦС

При эксплуатации серверной части «СЗИ от НСД «Блокхост-Сеть 4» под управлением ОС семейств Linux не предусматривается возможность взаимодействия с центром сертификации Microsoft CA напрямую.

Для возможности обращения к центру сертификации Microsoft CA серверной части «C3И от HCД «Блокхост-Сеть 4» под управлением OC Linux с целью выпуска сертификатов Microsoft CA необходимо выбрать одну из клиентских рабочих станций под управлением OC Windows и назначить ее прокси-клиентом, через который будет происходить взаимодействие с центром сертификации Microsoft CA.

Установка флага *Указать прокси-клиент для представления доступа* (рисунок 4.15) позволяет выбрать клиентскую рабочую станцию Блокхост-Сеть под управлением OC Windows для взаимодействием с центром сертификации Microsoft CA.



i

При обращении к центру сертификации Microsoft CA серверной части «СЗИ от НСД «Блокхост-Сеть 4» под управлением ОС Windows установка флага является опциональной.

🗙 Создание профиля Active Directory	×
Имя профиля	
Профиль 1]
Описание	
Введите описание профиля	
Указать прокси-клиент для предоставления доступа ③	
Для выпуска сертификатов необходимо выбрать клиент Блокхост- Сеть на ОС Windows (proxy-клиент). Он будет использоваться для взаимодействия с удостоверяющим центром Microsoft.	
Proxy-клиент должен удовлетворять следующим требованиям: - всегда быть онлайн (в противном случае управление токенами и сертификатами будет недоступно) - должен быть установлен компонент <u>RSAT: Active Directory</u> <u>Certificate Services Tools.</u>	
Выбрать клиент	
Создать Отмена	

Рисунок 4.15 – Добавление прокси-клиента

При этом прокси-клиент должен удовлетворять следующим требованиям:

– всегда быть в состоянии онлайн (для возможности выпуска сертификатов);

– на клиенте должен быть установлен компонент **RSAT Active Directory Certificate Services (AD CS) tools (<u>https://learn.microsoft.com/en-us/troubleshoot/windows-</u><u>server/system-management-components/remote-server-administration-tools</u>).**

По кнопке добавьте клиентскую рабочую станцию Блокхост-Сеть под управлением ОС Windows, которая будет использоваться для взаимодействия с центром сертификации Microsoft CA (рисунок 4.16).



Рисунок 4.16 – Выбор прокси-клиента

Введите наименование профиля, его описание и параметры сервисной учетной записи (имя пользователя и пароль) в соответствующих полях (рисунок 4.17).



🗙 Создание профиля Active Direc	tory			×
Имя профиля				
Профиль 1]
Описание				
Введите описание профиля				
🗹 Указать прокси-клиент для пр	едоставления до	оступа 🛈		
Прокси-клиент Windows 📲	W104 :			1
Каталог учетных записей	0			1
Active Directory				
pki.local				
Выпуск сертификатов				
Имя пользователя 🛈 serv	riceca			
Пароль •••	•••••			
КИ	менить]
Имя центра сертификации Micros	oft CA			
s09dc.pki.local\pki-S09DC-CA				
Сертификат агента регистрации -	Enrollment Ager	nt 🛈 C		
4ee2b7711c6db5e1c4b5878af618ff	ff8aa90fc8		\odot	
Шаблон сертификата для входа С	;			
SmartcardLogonTokensystem			•]
Таймаут ожидания при выпуске се	ертификата, сек		30]
Размер ключа, бит			1024 🌲]
🗌 Публиковать выдаваемые сер	тификаты в Acti	veDirector	y 🛈	
Co	оздать	C)тмена	

Рисунок 4.17 – Ввод данных для создания профиля

Дальнейшие действия по созданию профиля выпуска сертификата аналогичны описанным в разделе **Создание профиля Microsoft CA**.

Необходимо обратить внимание, что все шаги по выпуску и установке сертификата агента регистрации, описанные в разделе Создание профиля Microsoft CA выполняются на клиентской рабочей станции, выбранной в качестве прокси-клиента.

При необходимости, прокси-клиента возможно изменить или удалить с помощью контекстного меню (рисунок 4.18).

При удалении или изменении прокси-клиента все его настройки будут утеряны.

🗙 Создание профиля Active Directory		×
Имя профиля		
Профиль 1		1
Описание		1
Введите описание профиля		l
Указать прокси-клиент для предост	ставления доступа 🛈	l
Прокси-клиент Windows 🖬 W104	04 🛱 Заменить	l
Каталог учетных записей 🛈	🔟 Удалить	

Рисунок 4.18 – Изменение прокси-клиента

Флаг Публиковать выдаваемые сертификаты в Active Directory (рисунок 4.19) необходим для того, чтобы все выпускаемые сертификаты публиковались в Active Directory пользователя, который был указан при выпуске токена. Посмотреть их можно на домен-контроллере: Active Directory Users and Computers → Свойства пользователя → Published Certificates.

При отзыве токена через подсистему управления токенами, выпущенный сертификат автоматически удаляется из Active Directory пользователя (при отзыве через оснастку Windows этого не произойдет).



🔀 Создание профиля Active Directory	×
Имя профиля	
Профиль 1	
Описание	
Введите описание профиля	
🖌 Указать прокси-клиент для предоставления доступа ③	1
Прокси-клиент Windows 🔛 W104 :	1
Каталог учетных записей 🛈	
Active Directory	
pki.local	
Выпуск сертификатов	1
Имя пользователя 🙂 serviceca	
Пароль	
Изменить	
Имя центра сертификации Microsoft CA	
s09dc.pki.local\pki-S09DC-CA	
Сертификат агента регистрации - Enrollment Agent 🛈 Ĉ	
4ee2b7711c6db5e1c4b5878af618ffff8aa90fc8 O	
Шаблон сертификата для входа $ { m C} $	
SmartcardLogonTokensystem •	
Таймаут ожидания при выпуске сертификата, сек 30	
Размер ключа, бит 1024 🌲	
Публиковать выдаваемые сертификаты в ActiveDirectory ③	
Создать Отмена	

Рисунок 4.19 – Публиковать выдаваемые сертификаты в AD

5 Особенности при выпуске токена средствами подсистемы

При выпуске токена средствами подсистемы жизненного цикла токенов, с записью на него сертификата для входа пользователя или при использовании токена для входа по паролю, на токен записывается информация служебного характера (рисунок 5.1).

🔗 Единый Клиент JaCarta			
Единый Клие	нт JaCarta		Аладдин
	JaCarta		
JaCarta	Информация о токене РКІ		
	Операции с приложением		
	Сменить PIN-код	код <u>Создать запрос на</u>	
	Разблокировать PIN- код пользователя	ть	
	Ключи и сертификаты		
	6666\e015\000b\4653	0.19 Кбайт	
🔅 Настройки			
Переключиться в режим пользователя			

Рисунок 5.1 – Запись служебной информации при выпуске токена

Служебная информация на токене не подлежит удалению или редактированию. Указанные действия приведут к некорректной работе подсистемы с используемым токеном, и ошибкам при выполнении операций с ним.

Дальнейшие действия администратора по работе с подсистемой управления жизненным циклом токенов описаны в документе «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 5. Управление токенами».

6 Настройка прозрачного входа в RDGW

Удалённое подключение к рабочей станции осуществляется через RDGW (защищённый RDP), используется аутентификация на шлюзе удалённых рабочих столов по сертификату, сохранённому на токене.

Прозрачный вход возможен только в случае разрешённого для пользователя типа входа «Аутентификация Windows» в разделе клиентской политики «Управление входом в ОС» (подробное описание приведено в документе «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 1. Управление политиками»).

Для настройки прозрачного входа необходимо выполнить следующие действия:

- 1) Выполнить запуск *mstsc* и настроить RDGW вход.
- 2) Сохранить настройки в отдельный файл, например, *rdgw.rdp*.
- 3) Проверить возможность подключения по RDGW.
- 4) Открыть сохранённый файл *rdgw.rdp* в блокноте и добавить параметры:

promptcredentialonce:i:0
prompt for credentials on client:i:0
prompt for credentials:i:0

где:

promptcredentialonce:i:0 – соответствует снятию флага «использовать мои учётные данные шлюза для удалённого компьютера»;

prompt for credentials on client:i:0 prompt for credentials:i:0

отключают запрос данных локальной станции, заставляя искать сохранённые credentials.

5) Сохранить файл *rdgw.rdp*.

6) Сохранить credentials входа через с указанием полного имени рабочей станции, включая суффикс домена (например, gis.lan или da.lan):

cmdkey /add:targetname /user:username /pass:password

Например:

cmdkey /add:test.da.lan /user:testuser /pass:TestPassw0rd

В результате данной настройки пользователь вводит ПИН-код от смарт-карты для аутентификации на шлюзе рабочих столов по сертификату и подключается к удалённой рабочей станции без дополнительного ввода логина и пароля.



7 Настройка входа по сертификатам ЦС Microsoft CA в OC Linux

Перед настройкой входа по сертификатам на рабочие станции под управлением ОС семейства Linux необходимо убедиться в том, что на рабочих станциях установлены все последние обновления ОС и что на рабочей станции установлена клиентская часть СЗИ от НСД «Блокхост-Сеть 4».

Установка клиентской части СЗИ на рабочие станции под управлением ОС семейства Linux описана в документе «СЗИ от НСД «Блокхост-Сеть 4». Руководство по инсталляции в ОС Linux».

7.1 Приоритет проверок средств аутентификации при входе

При входе пользователя в ОС семейства Linux действует следующая очередность проверок предъявляемых пользователем средств аутентификации по убыванию приоритета: вход по сертификату, вход по БВПП, вход по паролю:

1) При предъявлении пользователем токена, в первую очередь выполняется проверка на наличие на устройстве сертификата для входа:

если сертификат для входа присутствует на токене (вне зависимости от истечения срока действия сертификата, наличия возможности безопасного входа по паролю), будет осуществлена попытка входа по сертификату.

2) При отсутствии на предъявляемом токене сертификата для входа, выполняется проверка на наличие на устройстве возможности безопасного входа по паролю:

если безопасный вход по паролю возможен для пользователя, будет осуществлена попытка входа по паролю на токене.

3) В случае невозможности входа по сертификату и по паролю на токене, пользователь может воспользоваться входом по паролю без предъявления токена, при этом предъявляемое для входа устройство необходимо извлечь.

7.2 Ввод рабочей станции ОС Linux в домен AD

7.2.1 Ввод рабочей станции под управлением ОС Альт в домен Active Directory

Перед вводом рабочей станции в домен, необходимо предварительно убедиться в правильности настроек сети (домен и все вводимые в него рабочие станции находятся в одной виртуальной подсети) и в отсутствии расхождения по времени между доменом и рабочей станцией, которая вводится в домен.



Ввод рабочей станции под управлением ОС Альт в домен Active Directory может быть выполнен только одним способом с использованием инструментария sssd.

Подробное описание ввода в домен Active Directory рабочей станции под управлением OC Альт доступно на сайте справочного центра Альт https://www.altlinux.org/ActiveDirectory/Login.

Для ввода в домен рабочей станции в ОС Альт необходимо последовательно выполнить следующие действия:

1) Скачать и установить все необходимые для работы пакеты:

sudo apt-get install task-auth-ad-sssd samba-client sssd-ad

2) Если используется домен, оканчивающийся на «.local», выполнить следующую команду:

sudo chkconfig avahi-daemon off
sudo reboot

3) В *Центре управления системой* перейти в раздел **Пользователи** → **Аутентификация**, выбрать пункт **Домен Active Directory** и заполнить поля (рисунок 7.1).

	Центр управл
авная 📃 Режим экс	перта 🗙 Выход
🔘 Локальная база п	юльзователей
О Ломен AIT Linux и	na Astra Linux Directory
Ломен: PKLI OCAI	and place check birdecery
Komunaaaaa ay	
Кэшировать ау	тентификацию при недоступности сервера домена
Домен Active Dire	ctory
Домен:	PKI.LOCAL
Рабочая группа:	PKI
Имя компьютера:	ALT
	N
🔿 Домен FreelPA	\$
 Домен FreeIPA Домен: 	pki.local
 Домен FreeIPA Домен: Имя компьютера: 	pki.local alt
 Домен FreeIPA Домен: Имя компьютера: 	pki.local alt
О Домен FreeIPA Домен: Имя компьютера: Внимание!	pki.local alt
О Домен FreeIPA Домен: Имя компьютера: Внимание! Изменение домена	ркi.local alt заработает только после перезагрузки компьютера
О Домен FreeIPA Домен: Имя компьютера: Внимание! Изменение домена	ркi.local alt заработает только после перезагрузки компьютера

Рисунок 7.1 – Заполнение полей для ввода в домен AD

4) Нажать кнопку Применить.

7.2.2 Ввод рабочей станции под управлением ОС Astra Linux в домен Active Directory

- **i**
- Перед вводом рабочей станции в домен, необходимо предварительно убедиться в **правильности настроек сети** (домен и все вводимые в него рабочие станции находятся в одной виртуальной подсети) и **в отсутствии расхождения по времени** между доменом и рабочей станцией, которая вводится в домен.

Ввод рабочей станции под управлением Astra Linux в домен Active Directory может быть выполнен с использованием инструментария winbind.

Подробное описание ввода в домен Active Directory рабочей станции под управлением OC Astra Linux каждым из способов доступно на сайте справочного центра Astra Linux <u>https://wiki.astralinux.ru/pages/viewpage.action?pageId=27361515</u>.

Для ввода в домен рабочей станции в OC Astra Linux необходимо последовательно выполнить следующие действия:

1) Скачать и установить все необходимые для работы пакеты:

sudo apt install fly-admin-ad-client

2) Открыть **Панель управления**:



Рисунок 7.2 – Открытие панели управления

3) Выбрать раздел *Сеть* → *Настройка клиента Active Directory:*



Рисунок 7.3 – Настройка клиента Active Directory



4) Заполнить все поля и нажать кнопку **Подключиться**:

💂 Настройка Active Directory 💶 🗢 🗙								
		Опции						
	Контроллер домена	dc01]			
	Рабочая группа	не обязательно]			
	Имя домена	example.com]			
	Сервер времени	не обязательно]			
	Администратор домена	Администратор]			
	Пароль	••••••]			
	Статус		Подклю	читься	1			
	astra-winbind -i сервис недоступен							

Рисунок 7.4 – Заполнение полей и подключение

7.2.3 Ввод рабочей станции под управлением РЕД ОС в домен Active Directory

Перед вводом рабочей станции в домен, необходимо предварительно убедиться в правильности настроек сети (домен и все вводимые в него рабочие станции находятся в одной виртуальной подсети) и в отсутствии расхождения по времени между доменом и рабочей станцией, которая вводится в домен.

Подробное описание ввода в домен Active Directory рабочей станции под управлением РЕД ОС доступно на сайте справочного центра РЕД ОС <u>https://redos.red-soft.ru/base/arm/arm-domen/arm-msad/</u>.

Для ввода в домен рабочей станции в РЕД ОС необходимо последовательно выполнить следующие действия:

1) Задать имя клиентского компьютера следующей командой:

hostnamectl set-hostname <Имя компьютера>.<домен>

при этом, имя клиентского компьютера обязательно должно содержать *win.redos*.

2) В файле /etc/hosts указать:

127.0.0.1 <Имя компьютера>.<домен> <Имя компьютера>

3) Проверить доступность клиентского компьютера командой:

ping <Имя компьютера>.<домен>

4) Установить графический инструмент **join-to-domain** для ввода рабочей станции в домен:

dnf update join-to-domain

5) После установки пакет будет доступен в графическом меню *Главное меню* → *Системные* → *Ввод ПК в домен*.

6) Для ввода рабочей станции в РЕД ОС в домен Active Directory необходимо выполнить запуск инструмента, введя пароль от пользователя **root**.

7) После успешной аутентификации откроется окно выбора типа домена, выберите пункт *Домен Windows/Samba*:

(ЭВ	вод в домен (от суперпользова 🗵						
	Выбе	ерите в какой домен добавить ПК						
		Домен						
	🔘 Домен Windows/Samba							
	О Домен IPA							
		Cancel OK						

Рисунок 7.5 – Выбор домена

8) После успешной аутентификации откроется основное окно, в котором необходимо указать имя домена, имя и пароль администратора и нажать кнопку **Да**:



🔹 Ввод в домен (от суперпользователя) 😑 🕀 🛞							
Ввод компьютера в домен							
Имя домена:	win.redos						
Имя компьютера:	vm521						
Имя администратора домена:	admin						
Пароль администратора:	••••••						
	Отмена Да						

Рисунок 7.6 – Ввод компьютера в домен

7.3 Порядок настройки для входа по сертификатам в ОС Linux

Для возможности аутентификации пользователя на клиентской рабочей станции под управлением СЗИ от НСД «Блокхост-Сеть 4» с использованием цифрового сертификата в ОС Linux необходимо выполнить следующие действия на клиентской рабочей станции:

1) Установить корневые сертификаты домена Active Directory.

2) Запустить задачу по настройке входа по сертификату через подсистему развертывания.

7.3.1 Экспорт корневого сертификата AD

Для установки корневого сертификата домена Active Directory необходимо перейти к настройкам центра сертификации и выполнить следующие действия:

1) В командной строке выполнить команду *ттс*.

2) Добавить оснастку **Сертификаты** для локального компьютера (**Файл** → **Добавить или удалить оснастку…**):



онастка	Поставшик	^		Корень консоли	ı. I	Изменить расширения.
MONISTON IR-Gero	Microsoft C			🛱 Сертификат	ы (локальный ко	
Монитор бранлм	Microsoft C					Удалить
Общие папки	Microsoft C					
Папка	Корпораци					Вверх
Планировщик за	(с) Корпора					
Просмотр событий	(с) Корпора		Deferrer			Вниз
🕽 Редактор объек	Microsoft C		дооавить >			
🕻 Результирующа	Microsoft C					
Сертификаты	Корпораци					
Осистемный мони	Корпораци					
🗼 Службы	Microsoft C					
• Службы компоне	Microsoft C					
Ссылка на веб-р	Корпораци	~		<	>	Дополнительно

Рисунок 7.7 – Добавление оснастки «Сертификаты»

3) Перейти в **Доверенные корневые центры сертификации**, найти корневой сертификат центра сертификации и экспортировать его в Base64 (*контекстное меню* → **Все задачи** → **Экспорт**).



a)



СЗИ от НСД «Блокхост-Сеть 4»
Руководство администратора безопасности. Часть 3
Настройка подсистемы управления токенами, ЦС Microsoft CA

Формат экспортиру Сертификаты і	мого файла огут быть экспортированы	в различных фор	матах.	
Выберите ф орг	ат, который вы хотите испо	ользовать:		
🔾 Файлы Х	509 (.CER) в <u>к</u> одировке DEF	ι		
💿 Файлы Х	509 (.CER) в к <u>о</u> дировке Ваз	e-64		
() <u>С</u> тандар	r Cryptographic Message Syn	tax - сертификат	ы PKCS #7 (.	p7b)
<u>В</u> клк	нить по возможности все се	ртификаты в пут	ъ сертифика	ации
<u>Ф</u> айл об	ена личной информацией - І	PKCS #12 (.PFX)		
Вклк	нить по возможности все се	ртификаты в пут	ъ сертифика	ниции
<u>У</u> дал	ить закрытый ключ после у	спешного экспор	та	
Эксп	ртировать вс <u>е</u> расширеннь	е свойства		
Вклк	нить конфиденциальность	сертификата		
() <u>Х</u> ранили	це сериализованных сертиф	икатов (.SST)		
		_		
			<u>Да</u> лее	Отм

Рисунок 7.8 – Экспорт корневого сертификата центра сертификации

4) Записать экспортируемый сертификат на переносное устройство для установки на клиентской рабочей станции.

5) На клиентской рабочей станции под управлением СЗИ от НСД «Блокхост-Сеть 4» для сохранения сертификата центра сертификации создать каталог /*etc/certs/:*

sudo mkdir /etc/certs

6) Скопировать в каталог /*etc/certs*/ сертификат центра сертификации (root_base64.cer):

sudo ср /<директория хранения сертификата> /etc/certs

7.3.2 Запуск задачи по настройке входа по сертификату через подсистему развертывания

Для создания задачи по настройке входа по сертификату на клиентских рабочих станциях откройте консоль управления Блокхост-Сеть перейдите по кнопке вкладку *Задачи*, раскройте меню создания задач по кнопке и выберите пункт *Настройка входа по сертификатам* (рисунок 7.9).

Х Блокхо	ост-Сеть 4						
충 Pa	азвёртывание				-		×
	soeproiounne						
s\$a	Агенты Пакеты установки	Задачи					
-	+						С
70	к⁰я Установка агента развертывания		▲ Тип	oc	Статус		
	🔄 Установка программы	ренной загрузки SafeNode System	Loader установка программы		завершено		
	 Удаление программы Перезагрузка компьютеров Выполнение скрипта 	вания 4.4.16789.29890 иля по требованию 4.4.16789.2989	установка агента развертывания О установка программы	Windows Windows	ожидает выпо ожидает выпо	лнения лнения	I
	Взятие под управление	4.16789.29890	установка программы	Windows	ожидает выпо	лнения	
	🕅 Поиск компьютеров без СЗИ						
(🛐 Настройка входа по сертификатам						

Рисунок 7.9 – Выбор задачи настройки входа по сертификатам

В открывшемся окне создания задачи настройки входа по сертификатам (рисунок 7.10) нажмите кнопку • Выбрать для перехода к окну выбора домена.

🗙 Создание задачи на настройку входа по сертификатам					
Задайте настройки домена					
Домен:	🕀 Выбрать				
Контроллер домена: 🛈					

Рисунок 7.10 – Задание настроек домена

Выберите нужный домен (рисунок 7.11 а) или, при отсутствии необходимого домена в списке, добавьте его по ссылке • Добавить домен (рисунок 7.11 б) и нажмите **ОК**.

🔀 Выбор домена/директории (OU)	×
💠 pki.local (AD)	
Добавить домен	
	Отмена



🗶 Добавление доме	на	×	
Active Directory	FreeIPA		
Имя домена			
pki.local1			
Имя пользователя			
user@domain			
Пароль			
•••••			
	Подключиться		

б)

Рисунок 7.11 – Выбор домена

Домены во вкладке **Домены** подразделяются на:

- *системные* домены, которые добавляются в список доменов автоматически. Подключение к системному домену (при раскрытии дерева или по двойному щелчку) происходит из-под текущей учетной записи или, в случае неудачи, запрашивается логин/пароль для подключения.

– *пользовательские* домены, которые добавляются по кнопке ^О ^{Добавить домен}. При подключении к пользовательскому домену всегда запрашивается логин/пароль для подключения (попытка подключения из-под текущей учетной записи не выполняется).

После выбора домена нажмите кнопку Далее (рисунок 7.12).



60

да по сертификатам		×
pki.local 🗄		
AD v		
s09dc.pki.local		
	Далее	Отмена
	да по сертификатам pki.local : AD • s09dc.pki.local	pki.local : AD • s09dc.pki.local

Рисунок 7.12 – Отображение выбранного домена

Выберите в списке те рабочие станции, на которых необходимо выполнить настройку входа по сертификатам, и нажмите кнопку **Далее** (рисунок 7.13).

🔀 Создание задачи на настройку входа по сертификатам				
Выберите к	омпьютеры			
Поиск			c	
🛷 Выбрать в	асё 🗍 Снять всё			
Имя	▲ IP-адрес	oc		
🔽 🛼 w09	w13.pki 10.72.9.62	Windows 10 64-bit		



В следующем окне (рисунок 7.14 а) по кнопке **Добавить** добавьте корневой сертификат домена Active Directory (экспорт подробно описан в разделе **«Экспорт корневого**



сертификата AD»). При необходимости воспользуйтесь инструкцией по установке корневого сертификата доступной по кнопке *К подробной инструкции* (рисунок 7.14 б).

Abiopure kopieesia cegruidpukaria JUL Affar proteode un copieesio cegruidpukaria Julia Active Directory ieodoxguno nepetiru i : a osuangino if cipore selanoanitra scoanary mmi : obaansi courciny Cegruidpukaria Julia nokananoro kommorepa(bain – "Gofasaris kun yganita : obaansi courciny Cegruidpukaria Julia nokananoro kommorepa(bain – "Gofasaris kun yganita : obaansi courciny Cegruidpukaria Julia nokananoro kommorepa(bain – "Gofasaris kun yganita : obaansi courciny Cegruidpukaria Julia nokananoro kommorepa(bain – "Gofasaris : obaansi courciny Cegruidpukaria Julia : obaansi courciny Cegruidpukaria Julia : obaansi courciny Cegruidpukaria : obaansi courciny Cegruidpuk	Co	здание задачи на нас	тройку входа по с	ертификата	м
Да установки корневого сертификата домена Асtive Directory необходимо перейти к настройкам центра сертификаты для локального компьютера(Файл – Добавить или удалить оснастку) <i>к</i> подробной инструкции	Выберите корневые сер	гификаты УЦ			
оснастку) Клодробной инструкции © Добавить	Для установки корневого с настройкам центра сертиф • В командной строке вып • Добавить оснастку Серти	ертификата домена Active Dire икации и выполнить следующи олнить команду mmc фикаты для локального компы	ctory необходимо перейти ие действия: ютера(Файл → Добавить и	1 к ли удалить	
О добавить В добавить Пазад Далее Отмена Далее Отмена В Создание задачи на настроику ехода по сертификата Создание задачи на настроику ехода по сертификата Казад Отмена Далее Отмена Создание задачи на настроику ехода по сертификата Казар Создание задачи на настроику ехода по сертификата Казар Создание задачи на настроику ехода по сертификата Создание задачи на настроику ехода по сертификата Создание задачи на настроику ехода по сертификата Ала установок корневые сертификата домена Астие Directory необходимо перейти к настроику сертификата Создание задачи на настроику ехода по сертификата Ала установок корневые сертификата домена Астие Directory необходимо перейти к настроику сертификата (растисти сертификата) Создание задачи на настроику ехода по сертификата Ала установок корневые сертификата домена Астие Directory необходимо перейти к настроику сертификата (растисти сертификата) Создание задачи сертификата (растисти сертификата) Отмена Создание задачи сертификата (растисти сертификата) Создание задачи сертификата) Отмена Создание задачи сертификата (растисти сертификата) Создание задачи сертификата) Отмена Создание задачи сертификата) С	оснастку)		• • • • • •		К подробной инструкции
Сортификаты отсутствуют Сортификаты отсутствуют Добавить Назад Далее Отмена А Алее Отмена А Создание задачи на настройку входа по сертификатам В Создание задачи на настройку входа по сертификатами В Создание задачи на настройкатами на настройку входа по сертификатами В Создание задачи на настройку входа по сертифика	Добавить				
Содание задачи на настроику входа по сертификата Азар Создание задачи на настроику входа по сертификата Создание задачи на настроику входа по сертификата систорија Создание задачи на настроику вободано перейти к коронеми нерти сертификата дав покаленого компанотера(Файл – Добанть или уданить систорија Сосанација Созданите сертификата дав покаленого компанотера(Файл – Добанать или уданить систорија Созданите сертификата дав покаленого компанотера(Файл – Добанать или уданить систорија Созданите сертификата и дав покаленого компанотера(Файл – Добанать или уданить систорија Созданите сертификата и дав покаленого компанотера(Файл – Добанать или уданить систорија Созданите сертификата и дав покаленото компанотера(Файл – Добанать или уданить систорија Созданите сертификата и дав покаленото компанотера(Файл – Добанать или уданить систорија Созданите сертификата и дав покаленото компанотера(Файл – Добанать или уданить систорија Созданите сертификата и дав покаленото компанотера(Файл – Добанать или уданить систорија Созданите сертификата и дав покаленото компанотера(Файл – Добанать или уданить систорија Созданите сертификата и дав покаленото компанотера(Файл – Добанать или уданить систорија Созданите сертификата и дав покаленото компанотера (Файл – Добанать или уданить систорија Созданите сертификата и дав покаленото компанотера (Файл – Добанать или уданить систорија Созданите сертификата и дав покаленото компанотера (Файл – Добанать или уданить систорија Созданите сертификата и дав покаленото компанотера (Файл – Добанать или уданить					
Сронфикаты отсутствуют Добавить Назад Дале Отмена Адае Создание задачи на настроику входа по сертификата Создание задачи на настроику входа на сертификата создание задачи на настроику входа на сертификата создание задачи на настроиката на настроику входа на сертификата создание задачи на настроику вход					
Добавить Назад Далее Отмена а) Создание задачи на настроику входа по сертификатам Создание задачи на коланду посертификата домена Астіче Directory необходимо перейти к настройкам центра сертификата домена Астіче Directory необходимо перейти к подробной инструкции Соравить сертификата домена Астиче Добавить и и и удалить симати сертификата домена Астиче Добавить и и и удалить симати сертификата домена Астиче Добавить и и удалить сим					
Назад Далее Отмена а) Создание задачи на настроику входа по сертификатам Создание сертификата домена Active Directory необходимо перейти к настройкам центра сертификата домена Active Directory необходимо перейти к настройкам центра сертификата домена Active Directory необходимо перейти к настройкам центра сертификата домена Асtive Directory необходимо нерейти к настройкам центра сертификата домена Асtive Directory необходимо нерейти к настройкам центра сертификата домена Асtive Directory необходимо перейти к настройкам центра сертификата домена Асtive Directory необходи Сертификата серти сертификата сертификата серти се		Сертифи	икаты отсутствуют Добавить		
Назад Далее Отмена а) Создание задачи на настроику входа по сертификатам Создание задачи на настроику входа по сертификатам Создание задачи на настроику входа по сертификатам Создание задачи на настроику входа по сертификата Создание задачи по сертификата домена Астіче Directory необходимо перейти к настройкам центра сертификаты для локального компьютера(Файл – Добавить кли удалить ссизастку) Собавить К подробной инструкци Содавить Удалить татель Кому вида – Сертибнай номер Амістантизни до Хиш См с ркі-500. 12 вел/ності номер Хиш					
Назад Далее Отмена а) Создание задачи на настроику входа по сертификатам Создание задачи на настроику входа по сертификатам Коловки корневые сертификаты УЦ Для установки корневого сертификата домена Асtive Directory необходимо перейти к настройкам центра сертификаты УЦ Для установки корневого сертификата домена Асtive Directory необходимо перейти к настройкам центра сертификаты для локального компьютера(Файл – Добавить или удалить следобной инструкци • добавить селастку) К подробной инструкци • Добавить Удалить Кому выда • Серийский номер Действителен до Кому выда • Серийский номер Действителен до Хии N = pki-509 12 деа74b2b3c7 30.03.200 6139afd2bbda259b35434aa6a46bb917bcec667d					
а) Создание задачи на настройку входа по сертификатам Создание задачи на настройку входа по сертификатам Создание задачи на настройку входа по сертификатам Анберите корневые сертификаты УЦ Для установки корневого сертификата домена Active Directory необходимо перейти к настройкам центра сертификаци и выполнить следующие действия: • В командной строке выполнить команду mmc • Добавить оснастку: Сертификаты для локального компьютера(Файл – Добавить или удалить оснастку) • Добавить Удалить К подробной инструкци С добавить Кому вида • Серпіный номер Действителен до Хиш СN = pki-S09 CN = pki-S090 12аеа74b2b3c7 30.03.2040 6139afd2bbda259b35434aa6a46bb917bcec667d			Назал		Отмена
а) <u>Создание задачи на настройку входа по сертификата</u> выберите корневые сертификаты УЦ Для установки корневого сертификата домена Асtive Directory необходимо перейти к настройкам центра сертификации и выполнить следующие действия: • В командной строке выполнить команду mmc • Добавить оснастку Сертификаты для локального компьютера(Файл – Добавить или удалить сивстку) К подробной инструкции Ф Добавить Удалить настель Кому вида – Сертібний номер Действияен до Хии N = pki-509 CN = pki-5090 12аеа74b2b3c7 30.03.2040 6139afd2bbda259b35434aa6a46bb917bcec667d			Пазад		
Создание задачи на настройку входа по сертификатам выберите корневые сертификаты УЦ Для установки корневого сертификата домена Active Directory необходимо перейти к настройкам центра сертификации выполнить следующие действия: • В командной строке выполнить команду mmc • Добавить оснастку Сертификаты для локального компьютера(Файл Добавить или удалить оснастку) К подробной инструкци © Добавить Удалить застель Кому видан + Сертібний комер Действителен до Хиш N = pki-509 CN = pki-5090 12aea74b2b3c7 30.03.200 6139afd2bbda259b35434aa6a46bb917bcec667d			a)		
Создание задачи на настроику входа по сертификатам ыберите корневые сертификаты УЦ Для установки корневого сертификата домена Active Directory необходимо перейти к настройкам центра сертификации и выполнить следующие действия: • В командной строис выполнить команду mmc • Добавить оснастку Сертификаты для локального компьютера(Файл — Добавить или удалить оснастку) К подробной инструкци © Добавить Вому выдам + Серийный номер Действителен до Хиш N = pki-509 CN = pki-509D 12аеа74b2b3c7 30.03.2040 6139afd2bbda259b35434aa6a46bb917bcec667d			,		
ыберите корневые сертификаты УЦ Для установки корневого сертификата домена Active Directory необходимо перейти к настройкам центра сертификации и выполнить следующие действия: • В командной строке выполнить команду mmc • Добавить оснастку Сертификаты для локального компьютера(Файл — Добавить или удалить оснастку) К подробной инструкци © Добавить Удалить задатель Кому видан + Сертиний номер Действителен до Хиш N = pki-S09 CN = pki-S09D 12aea74b2b3c7 30.03.2040 6139afd2bbda259b35434aa6a46bb917bcec667d	60	здание задачи на нас	троику входа по с	ертификата	м
Для установки корневого сертификата домена Асtive Directory необходимо перейти к настройкам центра сертификации и выполнить следующие действия: • В командной строке выполнить команду mmc • Добавить оснастку: Сертификаты для локального компьютера(Файл – Добавить или удалить оснастку) Кондробной инструкци Ф Добавить Удалить Іздатель Кому вмдан • Серліный номер Действителен до Хиш CN = pki-S09 CN = pki-S09D 12aea74b2b3c7 30.03.2040 6139afd2bbda259b35434aa6a46bb917bcec667d	выберите корневые серт	ификаты УЦ			
 Э. Добавить Удалить тадатель Кому выдан - Серийный номер Действителен до Хэш CN = pki-S09 CN = pki-S09D 12aea74b2b3c7 30.03.2040 6139afd2bbda259b35434aa6a46bb917bcec667d 	Для установки корневого с настройкам центра сертиф в командной строке вып "Добавить оснастку Серти оснастку)	ертификата домена Active Dire икации и выполнить следующ олнить команду mmc фикаты для локального компь	ctory необходимо перейт ие действия: ютера(Файл — Добавить и	и к или удалить	К подробной инструкции
 Эдотавить					
Iздатель Кому выдан - Серийный номер Действителен до Хэш N = pki-S09 CN = pki-S09D 12aea74b2b3c7 30.03.2040 6139afd2bbda259b35434aa6a46bb917bcec667d	🕙 Добавить 🛛 Удалить				
IN = pki-509 CN = pki-509D 12aea74b2b3c7 30.03.2040 6139afd2bbda259b35434aa6a46bb917bcec667d	іздатель Кому выдан	 Серийный номер. Действи 	ителен до Хэш		
	CN = pki-S09 CN = pki-S09	D 12aea74b2b3c7 30.03.2	040 6139afd2bbda	259b35434aa6a46	bb917bcec667d
	era: 1				
ere 1					
iero: 1			Назад	Далее	Отмена
его: 1 Назад Далее Отмена					
его: 1 Назад Далее Отмена			б)		

Рисунок 7.14 – Добавление корневого сертификата

В следующем окне выберите из списка производителя смарт-карты для которого будет выполняться настройка входа по сертификатам (рисунок 7.15).

При настройке двухфакторной аутентификации драйвера смарт-карты могут конфликтовать с драйверами других производителей в том числе и системными. Это может привести к невозможности входа с использованием сертификата. Рекомендуется выполнять настройку с установленным параметром Использовать драйвера только для выбранного производителя смарткарты (рисунок 7.15 б).

X	Создание зад	ачи на настройку входа по с	ертификатам	
Выберите пр	оизводителя смарт-карть	1		
Производитель	смарт-карты	*		
Использова	ать драйвера только для выбр	анного производителя смарт-карт ③		
				0
		назад		Отмена



K	Создание зада	чи на настройку входа по се	ртификатам	×
Выберите пр	ооизводителя смарт-карты			
Производител	ь смарт-карты	PYTOKEH +		
🛃 Использов	ать драйвера только для выбран	ного производителя смарт-карт 🛈		
		Назад	Далее	Отмена

б)

Рисунок 7.15 – Выбор производителя смарт-карты



Задайте параметры планировщика запуска задачи (подробнее в документе «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора. Часть 2. Развертывание и аудит» в пункте **«Указание параметров планировщика задачи по установке агента»**), определите интервалы времени выполнения задачи (рисунок 7.16) и нажмите кнопку **Далее** для продолжения создания задачи по настройке входа по сертификатам.

K	Создание задачи	на настройку входа по с	ертификатам	×
Параметры выполн	вения			
Тип запуска:	Вручную			*
Временные интерв	алы выполнения			
Остановить, если з	адача выполняется дольше,	часы		2
		Назад	Далее	Отмена

Рисунок 7.16 – Определение параметров планировщика и временных интервалов выполнения задачи

Введите имя создаваемой задачи и нажмите кнопку Создать.

В результате во вкладке **Задачи** будет создана новая задача по настройке входа по сертификатам с заданными в ходе работы мастера создания задачи параметрами.

В зависимости от установленных параметров планировщика запуск задачи будет осуществлен автоматически или вручную.

Для запуска задачи вручную выделите нужную задачу в списке и нажмите в меню кнопку ^{Запустить} или нажмите кнопку **Запустить** в открывшейся панели справа (подробнее в документе «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора. Часть 2. Развертывание и аудит» в пункте **«Запуск задачи»**).

В результате выполнения задачи по настройке входа по сертификатам на всех указанных в списке рабочих станциях будет настроен вход по сертификатам для выбранного производителя смарт-карт.

7.4 Особенности при входе в ОС Альт по сертификатам MS СА

Для корректной работы входа в ОС Альт по сертификатам MS CA, выпущенными средствами СЗИ от НСД «Блокхост-Сеть 4», необходимо произвести следующие настройки:

1) Добавить служебную учетную запись Enrollment-агента в группу Cert Publishers через оснастку контроллера домена: *Active Directory Users and Computers* → *Свойства пользователя* → вкладка *Member Of*.



Рисунок 7.17 – Добавление служебной учетной записи в группу Cert Publishers

2) Установить флаг **Публиковать выдаваемые сертификаты в Active Directory** в настройках выпуска сертификатов консоли управления Блокхост-Сеть при создании

профиля: *Настройки → Выпуск сертификатов* → создание профиля *Microsoft СА* (рисунок 7.18).



🗙 Создание профиля Active Directory	×
Имя профиля	
Профиль1	I
Описание	I
Введите описание профиля	
🗹 Указать прокси-клиент для предоставления доступа 🛈	l
Прокси-клиент Windows 🖬 W104 :	l
Каталог учетных записей 😳	l
Active Directory	I
pki.local	l
Выпуск сертификатов	l
Имя пользователя 🛈 serviceca	I
Пароль •••••••••	I
Изменить	I
	I
Имя центра сертификации Microsoft CA	I
s09dc.pki.local\pki-S09DC-CA	I
Сертификат агента регистрации - Enrollment Agent 🛈 C	I
4ee2b7711c6db5e1c4b5878af618ffff8aa90fc8 💿	I
Шаблон сертификата для входа С	l
SmartcardLogonTokensystem 🔹	I
Таймаут ожидания при выпуске сертификата, сек 30	I
Размер ключа, бит 1024 🍦	
🗹 Публиковать выдаваемые сертификаты в ActiveDirectory 🛈	
Создать Отмена]

Рисунок 7.18 – Установка флага **Публиковать выдаваемые сертификаты в Active** Directory



3) Выдать токен для входа по управляемому сертификату с помощью консоли управления (см. документ «СЗИ от НСД «Блокхост-Сеть 4». Руководство администратора безопасности. Часть 5. Управление токенами»).

Все выпущенные сертификаты будут публиковаться в Active Directory пользователя, указанного при выпуске токена.

Просмотреть сертификаты можно на контроллере домена: в оснастке Active Directory Users and Computers выбрать View — Advanced Features, затем перейти в оснастке к Свойства пользователя — вкладка Published Certificates (рисунок 7.19).

Active Directory Users and Computers [s09dc.pki.local]	Name	Туре	Description						
Saved Queries	& admin	User							
pki.local	& Administrator	User	Built-in account for ad						
3 🖬 12	St Allowed RODC Password Re	Security Group	Members in this group of	C					
🔉 🛄 Builtin	St. Cert Publishers	Security Group	Members of this group .						
🖂 Computers	St. Cloneable Domain Controllers	Security Group	Members of this gro				Descenti		2 3
Domain Controllers	St. Denied RODC Password Repl	Security Group	Members in this gro			user1	Propertie	es	
ForeignSecurityPrincipals	St. DosAdmins	Security Group	DNS Administrators	Canadhi	6	mimmant	Casel	0.00	Remote control
LostAndFound	St. DnsUpdateProxy	Security Group	DNS clients who are	Remote [Deskton S	envices Pmfile	000	M+	Attribute Editor
Managed Service Accounts	St Domain Admins	Security Group	Designated administ	General	Address	Account	Profile	Telephones	Omanization
Program Data	R Domain Computers	Security Group	All workstations and	Published Ce	rtficates	Member Of	Password	Replication	Dial-in Object
Special	St Domain Controllerr	Security Group	All domain controlle			indition of	1 00011010	(spreater)	T commit T orders
þ 🧾 System	R Domain Guests	Security Group	All domain quests	List of X509	certficat	es published fo	the user a	ccount	
Users	B Domain Ukarr	Security Group	All domain urarr	Issued To	1	Issued By	Intende	d Purposes	Expiration
NTDS Quotas	Sectororise Admins	Security Group	Decidented administ	Juser1	1	pki-S09DC-CA	Smart C	ard Logon, C	05.05.20
IPM Devices	Senterprise Adminis	Security Group	Members of this are		N				
	Comprise Read-only Domai	Security Group	Members of this gro		45				
	Group Policy Creator Owners	Security Group	Members in this gro						
	a Guest	User	Built-in account for						
	a krbtgt	User	Key Distribution Cen						
	Reprotected Users	Security Group	Members of this gro						
	RAS and IAS Servers	Security Group	Servers in this group	<		111		1	>
	Read-only Domain Controllers	Security Group	Members of this gro					Constant of the second	C. 18. 1
	Schema Admins	Security Group	Designated administ					VIEW	Certricate
	ServiceCA2	User							
	👗 sky	User							
	🙎 tai	User							
	🔏 user1	User							
	🚨 user2	User		-			_		
	🐍 user3	User		Add from	Store	Add from File	Re	move	Copy to File
				1			50 m 20		

Рисунок 7.19 – Публикация сертификата в Active Directory

Также, список сертификатов можно получить через LDAP-запрос (для этого следует включить в список запрашиваемых атрибутов *userCertificate*).

После проведения настроек вход по ранее выданным токенам в ОС Альт будет невозможен. Для входа по ранее выданным токенам необходимо заново выпустить все токены, с помощью которых планируется аутентификация в ОС Альт или добавить выпущенный сертификат в *Published Certificates* вручную на контроллере домена или отправив соответствующий LDAP-запрос.

7.5 Особенности при входе в ОС Astra Linux с настроенным входом по сертификатам

Если рабочая станция под управлением OC Astra Linux введена в домен с использованием инструментария sssd и на рабочей станции настроен вход по сертификатам, при попытке входа по БВПП OC будет запрашивать ввод ПИН-кода повторно, так как токен настроен в /etc/krb5.conf.

Если вход по сертификатам больше планируется использовать, можно отключить токен, закомментировав в */etc/krb5.conf* строку:

pkinit_identities = PKCS11:module_name=/usr/lib/librtpkcs11ecp.so

где:

pkinit_identities – библиотека используемого токена.

В дальнейшем, при входе пользователя по БВПП, ПИН-код не будет запрашиваться повторно.



Необходимо учитывать, что данное действие приведет к невозможности входа пользователя по сертификату.

7.6 Удаление сертификата из Active Directory пользователя

Для удаления сертификата из Active Directory пользователя можно воспользоваться двумя способами:

1) Отозвать токен через консоль управления Блокхост-Сеть. При этом выпущенный ранее сертификат автоматически удаляется из Active Directory пользователя.



При отзыве через оснастку Windows сертификат не удаляется.

2) Удалить сертификат вручную на контроллере домена: Active Directory Users and Computers → Свойства пользователя → вкладка Published Certificates.



Если служебная учетная запись enrollment-агента будет исключена из *Cert Publishers*, при этом сохранен установленный флаг *Публиковать выдаваемые сертификаты в Active Directory*, то система при каждом выпуске/отзыве токена будет выдавать соответствующее предупреждение о невозможности опубликовать/удалить сертификат в Active Directory.

7.7 Настройка публикации списка отзыва сертификатов в ОС Linux

При установке серверной части СЗИ от НСД «Блокхост-Сеть 4» на рабочей станции под управлением ОС Linux при выпуске токена для входа по управляемому сертификату, в результате того, что в ОС Linux списки отзыва сертификатов распространяются по протоколу *Idap*, может возникнуть ошибка вида:



Рисунок 7.20 – Ошибка определения статуса отзыва сертификата

В этом случае, необходимо выполнить настройку публикации списка отзыва сертификатов по протоколу *http*.

(i) После выполнения настроек для публикации списка отзывов сертификатов по протоколу *http*, чтобы корректно определялся статус сертификата на токене, все выданные токены для входа по управляемому сертификату необходимо перевыпустить!

7.7.1 Настройки центра сертификации

Для настройки публикации списка отзыва сертификатов по протоколу *http* перейдите к настройкам центра сертификации и откройте оснастку *Certification Authority* (рисунок 7.21).



	Shortcut Tools	Administrative To	ools	_ 🗆 X	
F Home Share	View Manage			~ e	E
🔄 🕘 ⊽ 🕇 🔞 « Sys	stem and Security Administrative Tools	v c	Search Administr	rative Tools 🛛 🔎	
☆ Favorites	Name	Date modified	Туре	Size	5
Desktop	퉬 Terminal Services	22.08.2013 19:39	File folder		
🗼 Downloads	🛃 Active Directory Administrative Center	22.08.2013 3:50	Shortcut	2 KB	
🖳 Recent places	🛃 Active Directory Domains and Trusts	22.08.2013 10:55	Shortcut	2 KB	
	Active Directory Module for Windows Po	22.08.2013 10:55	Shortcut	2 KB	
👰 This PC	💦 Active Directory Sites and Services	22.08.2013 10:55	Shortcut	2 KB —	1
膧 Desktop 📃	🛃 Active Directory Users and Computers	22.08.2013 10:55	Shortcut	2 KB	
Documents	📝 ADSI Edit	22.08.2013 10:55	Shortcut	2 KB	
🗼 Downloads	ត Certification Authority	22.08.2013 10:56	Shortcut	2 KB	
🚺 Music	Component Services	22.08.2013 10:57	Shortcut	2 KB	
📔 Pictures	🛃 Computer Management	22.08.2013 10:54	Shortcut	2 KB	
🛃 Videos	🚼 Defragment and Optimize Drives	22.08.2013 10:47	Shortcut	2 KB	

Рисунок 7.21 – Выбор оснастки Certification Authority

Окно консоли будет выглядеть следующим образом:

<u>Б</u> с	ertsrv - [Certification Authority (Local)\p	oki-S09DC-CA]	_ 🗆 X
<u>F</u> ile <u>A</u> ction <u>V</u> iew <u>H</u> elp			
🗢 🄿 🖄 🗐 🖓			
Ertification Authority (Local)	Name		
🔈 🛃 pki-S09DC-CA	📔 Revoked Certificates		
	📔 Issued Certificates		
	📔 Pending Requests		
	📔 Failed Requests		
	🚞 Certificate Templates		

Рисунок 7.22 – Консоль центра сертификации

В левой части окна перейдите в свойства центра сертификации (*Properties*) по щелчку правой кнопки мыши (рисунок 7.23).



Рисунок 7.23 – Настройка свойств центра сертификации



Перейдите во вкладку *Extensions* (рисунок 7.24), выберите расширение *CRL Distribution Point (CDP)*.

pki-S09DC-CA Properties								
Enrollment Agents	Auditing	Recovery Agents Security						
General	Policy Mo	Policy Module Exit Module						
Extensions	Storage		Certificate M	lanagers	;			
Select extension:								
C:\Windows\system3 Idap:///CN= <catrun http://<serverdnsna file://<serverdnsna< td=""><td>2<mark>\CertSrv\CertB</mark> catedName><c ame>/CertEnroll. me>/CertEnroll/</c </td><td>nroll\<can RLNameSu /<caname> <caname></caname></caname></can </td><td>ame><crln ffix>,CN=<se ><crlnames <crlnames< td=""><td>ameSuff rverShor Suffix><d uffix><de< td=""><th>tNar Delta eltaC</th></de<></d </td></crlnames<></crlnames </se </crln </td></serverdnsna<></serverdnsna </catrun 	2 <mark>\CertSrv\CertB</mark> catedName> <c ame>/CertEnroll. me>/CertEnroll/</c 	nroll\ <can RLNameSu /<caname> <caname></caname></caname></can 	ame> <crln ffix>,CN=<se ><crlnames <crlnames< td=""><td>ameSuff rverShor Suffix><d uffix><de< td=""><th>tNar Delta eltaC</th></de<></d </td></crlnames<></crlnames </se </crln 	ameSuff rverShor Suffix> <d uffix><de< td=""><th>tNar Delta eltaC</th></de<></d 	tNar Delta eltaC			
< 111	< III >							
✓ Publish CRLs to thi	s location	A	<u>d</u> d	<u>R</u> emove	e			
Include in all CRLs when publishing ma	Include in all CRLs. Specifies where to publish in the Active Directory when publishing manually.							
Include in CRLs. Clients use this to find Delta CRL locations.								
Include in the CDP extension of issued certificates								
✓ Publish Delta CRLs	s to this location							
Include in the IDP extension of issued CRLs								
ОК	Cano	el	Apply	He	lp			

Рисунок 7.24 – Переход во вкладку *Extensions*

Нажмите кнопку **Добавить (Add)** для добавления настроек (рисунок 7.25), в поле **Location** введите строку:

http://<ServerDNSName>/crl/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl

и нажмите **ОК**.



Add Location	x
A location can be any valid URL or path. Enter an HTTP, LDAP, file addres or enter a UNC or local path. To insert a variable into the URL or path, selec the variable below and click Insert.	is, ct
Location:	
Variable: <caname> V Insert</caname>	
Description of selected variable:	
Used in URLs and paths Inserts the DNS name of the server Example location: http:// <serverdnsname>/CertEnroll/<caname><crln< td=""><td>la</td></crln<></caname></serverdnsname>	la
< III	>
OK Cancel	
a)	

Add Location X
A location can be any valid URL or path. Enter an HTTP, LDAP, file address, or enter a UNC or local path. To insert a variable into the URL or path, select the variable below and click Insert.
Location:
http:// <serverdnsname>/crldl/<caname><crlnamesuffix><deltacrlallc< td=""></deltacrlallc<></crlnamesuffix></caname></serverdnsname>
Variable:
<serverdnsname> V Insert</serverdnsname>
Description of selected variable: Used in URLs and paths Inserts the DNS name of the server Example location: http:// <serverdnsname>/CertEnroll/<caname><crlna< td=""></crlna<></caname></serverdnsname>
< III >
OK Cancel
б)

Рисунок 7.25 – Добавление места публикации списка отзывов

Установите флаги (рисунок 7.26) для включения созданной записи в выдаваемые сертификаты.



pki-S09DC-CA Properties ? X							
Enrollment Agents	Auditing	Recover	y Agents	Security			
General	Policy Mo	odule	Exit	Module			
Extensions	Storage		Certificate M	lanagers			
Select extension:							
CRL Distribution Point	(CDP)			~			
Specify locations from (CRL).	Specify locations from which users can obtain a certificate revocation list (CRL).						
C:\Windows\system3 Idap:///CN= <catrunc http://<serverdnsnar file://<serverdnsnar http://<serverdnsnar< td=""><td>2\CertSrv\CertE catedName><c ame>/CertEnroll me>/CertEnroll/ ame>/crldl/<ca< td=""><td>Enroll\<cana RLNameSuft /<caname>< <caname>< Name><crl< td=""><td>ame><crln fix>,CN=<se <crlnames CRLNameSi NameSuffix</crlnames </se </crln </td><td>ameSuffix><l rverShortNar Suffix><delta uffix><deltac •<deltacrla< td=""></deltacrla<></deltac </delta </l </td></crl<></caname></caname></cana </td></ca<></c </td></serverdnsnar<></serverdnsnar </serverdnsnar </catrunc 	2\CertSrv\CertE catedName> <c ame>/CertEnroll me>/CertEnroll/ ame>/crldl/<ca< td=""><td>Enroll\<cana RLNameSuft /<caname>< <caname>< Name><crl< td=""><td>ame><crln fix>,CN=<se <crlnames CRLNameSi NameSuffix</crlnames </se </crln </td><td>ameSuffix><l rverShortNar Suffix><delta uffix><deltac •<deltacrla< td=""></deltacrla<></deltac </delta </l </td></crl<></caname></caname></cana </td></ca<></c 	Enroll\ <cana RLNameSuft /<caname>< <caname>< Name><crl< td=""><td>ame><crln fix>,CN=<se <crlnames CRLNameSi NameSuffix</crlnames </se </crln </td><td>ameSuffix><l rverShortNar Suffix><delta uffix><deltac •<deltacrla< td=""></deltacrla<></deltac </delta </l </td></crl<></caname></caname></cana 	ame> <crln fix>,CN=<se <crlnames CRLNameSi NameSuffix</crlnames </se </crln 	ameSuffix> <l rverShortNar Suffix><delta uffix><deltac •<deltacrla< td=""></deltacrla<></deltac </delta </l 			
< 111				>			
Publish CRLs to this	slocation	Ad	d	<u>R</u> emove			
Include in all CRLs. Specifies where to publish in the Active Directory when publishing manually.							
Include in CRLs. Clients use this to find Delta CRL locations							
✓ Include in the CDP extension of issued certificates							
Publish Delta CRLs to this location							
Include in the IDP extension of issued CRLs							
OK	Canc	el	<u>A</u> pply	Help			

Рисунок 7.26 – Включение созданной записи в выдаваемые сертификаты

Отключите те же флаги для *Idap* протокола (рисунок 7.27).


р	?	x				
Enrollment Agents	Auditing Recovery Agents				urity	
General	Policy Mo	dule	Exit M	lodule		
Extensions	Storage		Certificate Ma	nager	s	
Select extension:						
CRL Distribution Point	t (CDP)				~	
Specify locations from (CRL).	which users car	n obtain a ce	rtificate revoc	ation li	st	
C:\Windows\system3	2\CertSrv\CertE	Enroll\ <cana< td=""><td>me><crlnar< td=""><td>neSuff</td><th>ix><l< th=""></l<></th></crlnar<></td></cana<>	me> <crlnar< td=""><td>neSuff</td><th>ix><l< th=""></l<></th></crlnar<>	neSuff	ix> <l< th=""></l<>	
Idap:///CN= <catrun< td=""><td>catedName><c< td=""><td>RLNameSuf</td><td>ix>,CN=<serv< td=""><td>/erSho</td><th>rtNar</th></serv<></td></c<></td></catrun<>	catedName> <c< td=""><td>RLNameSuf</td><td>ix>,CN=<serv< td=""><td>/erSho</td><th>rtNar</th></serv<></td></c<>	RLNameSuf	ix>,CN= <serv< td=""><td>/erSho</td><th>rtNar</th></serv<>	/erSho	rtNar	
file:// <serverdnsna file://ServerDNSNa http://ServerDNSNa</serverdnsna 	ame>/CertEnroll/ me>/CertEnroll/ ame>/crddl/ <ca1< td=""><td>/<caname> <caname>< Name><crl< td=""><td><crlnamesu CRLNameSuff NameSuffix><</crlnamesu </td><td>/ftx><l fix><d Delta(</d </l </td><th>Delta eltaC CRLA</th></crl<></caname></caname></td></ca1<>	/ <caname> <caname>< Name><crl< td=""><td><crlnamesu CRLNameSuff NameSuffix><</crlnamesu </td><td>/ftx><l fix><d Delta(</d </l </td><th>Delta eltaC CRLA</th></crl<></caname></caname>	<crlnamesu CRLNameSuff NameSuffix><</crlnamesu 	/ftx> <l fix><d Delta(</d </l 	Delta eltaC CRLA	
		Ad	d <u>F</u>	<u>R</u> emov	e	
Publish CRLs to thi	s location					
✓ Include in all CRLs when publishing ma	. Specifies when anually.	e to publish i	n the Active [)irecto	Ŋ	
Include in CRLs. C	lients use this to	find Delta C	RL locations.			
Include in the CDP	extension of iss	ued certifica	tes			
Publish Delta CRLs	Publish Delta CRI s to this location					
Include in the IDP extension of issued CKLs						
ОК	Canc	el	Apply	He	elp	

Рисунок 7.27 – Отключение в протоколе Idap

Нажмите кнопку **Добавить (Add)** для добавления места хранения выпускаемого списка отзывов (рисунок 7.28) и укажите в поле **Location** адрес:

\\s09dc\crldist\$\<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl

и нажмите **ОК**.



Add Location X						
A location can be any valid URL or path. Enter an HTTP, LDAP, file address, or enter a UNC or local path. To insert a variable into the URL or path, select the variable below and click Insert.						
Location:						
\\s09dc\crldist\$\ <caname><crlnamesuffix><deltacrlallowed>.crl</deltacrlallowed></crlnamesuffix></caname>						
Variable: <caname> V Insert</caname>						
Description of selected variable: Used in URLs and paths The name of the CA Example location: http:// <servername>/CertEnroll/<caname><crlnamest< td=""></crlnamest<></caname></servername>						
< III >						
OK Cancel						

Рисунок 7.28 – Добавление места хранения выпускаемого списка отзывов

Для добавленной записи установите следующие флаги (рисунок 7.29):

р	?	x					
Enrollment Agents	Auditing	Sec	urity				
General	Policy Mo	dule	Exit M	lodule			
Extensions	Storage		Certificate Ma	nagers	s		
Select extension:							
CRL Distribution Poin	t (CDP)				~		
Specify locations from (CRL).	which users can	obtain a ce	rtificate revoc	ation li	st		
Idap:///CN= <catrun http://<serverdnsna file://<serverdnsna http://<serverdnsna< td=""><td>catedName><cf ame>/CertEnroll/ me>/CertEnroll/< ame>/crldl/<can Name><cblnar< td=""><td>RLNameSuff (<caname>< (CaName>< lame><crl neSuffic><d< td=""><td>ix>,CN=<serv <crlnamesu CRLNameSuff NameSuffix>< ettaCBLAllow</crlnamesu </serv </td><th>verSho uffix><[fix><d DeltaC</d </th><th></th></d<></crl </caname></td></cblnar<></can </cf </td></serverdnsna<></serverdnsna </serverdnsna </catrun 	catedName> <cf ame>/CertEnroll/ me>/CertEnroll/< ame>/crldl/<can Name><cblnar< td=""><td>RLNameSuff (<caname>< (CaName>< lame><crl neSuffic><d< td=""><td>ix>,CN=<serv <crlnamesu CRLNameSuff NameSuffix>< ettaCBLAllow</crlnamesu </serv </td><th>verSho uffix><[fix><d DeltaC</d </th><th></th></d<></crl </caname></td></cblnar<></can </cf 	RLNameSuff (<caname>< (CaName>< lame><crl neSuffic><d< td=""><td>ix>,CN=<serv <crlnamesu CRLNameSuff NameSuffix>< ettaCBLAllow</crlnamesu </serv </td><th>verSho uffix><[fix><d DeltaC</d </th><th></th></d<></crl </caname>	ix>,CN= <serv <crlnamesu CRLNameSuff NameSuffix>< ettaCBLAllow</crlnamesu </serv 	verSho uffix><[fix> <d DeltaC</d 			
	Namezkonena	neounixixo	CILCINENION				
✓ Publish CRLs to thi	Add <u>R</u> emove						
Include in all CRLs when publishing ma	. Specifies where anually.	e to publish i	n the Active D)irecto	ry		
Include in CRLs. C	lients use this to f	find Delta Cl	RL locations.				
Include in the CDP	extension of issu	ued certificat	es				
Publish Detta CBI s to this location							
Dischale in the IDD extension of insured CDLs							
ОК	Cance	el	Apply	He	elp		

Рисунок 7.29 – Установка публикации в выбранной локации



Нажмите *Применить (Apply)*.

7.7.2 Настройки на контроллере домена

Перейдите к настройкам контроллера домена и откройте оснастку **DNS** (рисунок 7.30).

🖄 🍃 🔝 🖛 I			Shortcut Tools	Application Tools	Administra	ative Tools	_ □	x
File Home Sh	are	View	Manage	Manage				~ ?
(a) < ↑	Syst	em and Sec	urity 🕨 Admini	strative Tools	~ ¢	Search Administra	ative Tools	P
🔆 Favorites	^	Name	*		Date modified	Туре	Size	^
Desktop		🎓 Comp	oonent Services		22.08.2013 10:57	Shortcut	2 KB	
📜 Downloads		🛃 Comp	outer Managemei	nt	22.08.2013 10:54	Shortcut	2 KB	
🕮 Recent places		눩 Defrag	gment and Optin	nize Drives	22.08.2013 10:47	Shortcut	2 KB	
		<table-cell-rows> DHCP</table-cell-rows>			22.08.2013 10:45	Shortcut	2 KB	
👰 This PC		浅 DNS			22.08.2013 10:55	Shortcut	2 KB	_
膧 Desktop	=	🚼 Event	Viewer		22.08.2013 10:55	Shortcut	2 KB	. –
Documents	-	🚮 Group	Policy Manager	nent	22.08.2013 10:56	Shortcut	2 KB	
🐌 Downloads		濻 Intern	et Information Se	ervices (IIS) Manager	22.08.2013 10:50	Shortcut	2 KB	
🜗 Music		🔝 iscsi I	Initiator		22.08.2013 10:57	Shortcut	2 KB	
📔 Pictures		🛃 Local	Security Policy		22.08.2013 10:54	Shortcut	2 KB	
📑 Videos		🔊 Micro	soft Azure Servic	es	24.07.2014 8:02	Shortcut	2 KB	
📥 Local Disk (C:)		📷 ODBC	Data Sources (32	2-bit)	22.08.2013 3:56	Shortcut	2 KB	
		📷 ODBC	Data Sources (64	4-bit)	22.08.2013 10:59	Shortcut	2 KB	
📬 Network	\sim	💱 Online	e Responder Man	agement	22.08.2013 10:56	Shortcut	2 KB	\sim
37 items 1 item selec	ted 1	,20 KB					:	=

Рисунок 7.30 – Выбор оснастки DNS

Окно консоли будет выглядеть следующим образом:

å	DNS Manager								
File Action View Help	<u>F</u> ile <u>A</u> ction <u>V</u> iew <u>H</u> elp								
 DNS S09DC Forward Lookup Zones Reverse Lookup Zones Trust Points Conditional Forwarders Fill Global Logs 	Name Carlor Servition Servitio Servition Servition Servition Servition Servition Serv	Type Active Directory-Integrated Pr Active Directory-Integrated Pr	Status Running Running	DNSSEC Status Not Signed Not Signed					

Рисунок 7.31 – Консоль контроллера домена DNS

В левой части окна перейдите раскройте пункт *Forward Lookup Zones*, перейдите к домену и по щелчку правой кнопки мыши выберите *New Host* (рисунок 7.32).

🖹 DNS Manager 📃 🗖 🗙							
<u>File</u> <u>A</u> ction <u>V</u> iew	<u>File Action View Help</u>						
<							
🚊 DNS		Name	Туре	Data	Timest ^		
⊿ 📱 S09DC		📳 _msdcs					
⊿ 📔 Forward Loo	kup Zones	🚞 _sites					
⊳ 📴 _msdcs.p	oki.local	🚞 _tcp					
▷ C pki.lc ▷ C pki.lc ▷ C pki.lc	Update Se	rver Data File					
Trust Poi	Reload						
Conditio	New Host	(A or AAAA)	Start of Authority (SOA)	[1044], s09dc.pki.local., ho	static		
Global Lo	New Alias	(CNAME)	Name Server (NS)	s09dc.pki.local.	static		
	New Mail	Exchanger (MX)	Host (A)	192.168.209.143	15.06.2		
	New Dom	ain	Host (A)	10.72.9.2	14.06.2 =		
	New Dele	nation	Host (A)	10.72.9.3	09.07.2		
	Other Ne	u Deseude	Host (A)	10.72.9.2	static		
	Other Nev	v Records	Host (A)	192.168.209.143	static		
	DNSSEC	•	Host (A)	10.72.9.60	30.03.2		

Рисунок 7.32 – Переход к меню домена

В открывшемся окне (рисунок 7.33) введите наименование в поле *Name* и укажите адрес сервера Блокхост-Сеть в поле *IP address*.

New Host X
Name (uses parent domain name if blank):
Fully qualified domain name (FQDN): crl.pki.local.
I <u>P</u> address: 10.72.9.2
Create associated pointer (PTR) record
Allow any authenticated user to update DNS records with the same owner name
Add <u>H</u> ost Cancel



Перейдите в оснастку **IIS** (рисунок 7.34).



🖄 🍃 📗 🖛 I			Shortcut Tools	Application Tools	Administ	rative Tools	_ □	x
File Home Sh	are	View	Manage	Manage				~ ?
(a) (b) < ↑ (b) (c) Search Administrative Tools (c) Search Administrative Tools						٩		
🔆 Favorites	^	Name	•		Date modified	Туре	Size	<u> </u>
E Desktop		😹 Group	Policy Manager	nent	22.08.2013 10:56	Shortcut	2 KB	
\rm Downloads		濻 Intern	et Information Se	ervices (IIS) Manager	22.08.2013 10:50	Shortcut	2 KB	
🖫 Recent places		🔝 iscsi I	Initiator		22.08.2013 10:57	Shortcut	2 KB	
		🛃 Local	Security Policy		22.08.2013 10:54	Shortcut	2 KB	
🖳 This PC		🔊 Micro	soft Azure Servic	es	24.07.2014 8:02	Shortcut	2 KB	
膧 Desktop	=	📷 ODBC	Data Sources (32	2-bit)	22.08.2013 3:56	Shortcut	2 KB	
Documents		📷 ODBC	Data Sources (64	1-bit)	22.08.2013 10:59	Shortcut	2 KB	
ॊ Downloads		🛜 Online	e Responder Man	agement	22.08.2013 10:56	Shortcut	2 KB	≡

Рисунок 7.34 – Выбор оснастки ИS

Окно консоли будет выглядеть следующим образом:

8]	Internet Information Services (IIS) Manager	_ D X
🕥 🖣 🕨 Start Page		🐱 🛛 🔂 🕡 🕶
<u>F</u> ile <u>V</u> iew <u>H</u> elp		
Eile View Help Connections Connections Start Page SogDC (PKI\Administrator) SogDC (PKI\Administrator)	Moresoft Application Server Manager Recent connections Connection tasks Name Set SO9DC loc SO9DC loc Connect to localhost Connect to a server Connect to a server Connect to a site Connect to a site Connect to an application Its News Its News is disabled, click the Enable IIS News link to get the most recent online	Online resources IIS News and Information IIS Downloads IIS Forums TechNet MSDN ASP.NET News Microsoft Web Platform Enable IIS News e news.
Ready		

Рисунок 7.35 – Консоль контроллера домена ///

В левой части окна раскройте контроллер домена, перейдите к пункту **Sites** → **Default Web Site** и по щелчку правой кнопки мыши выберите **Add Virtual Directory** (рисунок 7.36).



Internet Information Services (IIS) Manager								
SogDC → Sites → Default Web Site → Sites → Sites → Default Web Site → Sites → Sites → Default Web Site → Sites → Sites → Sites → Sites → Sites								
File View Help								
Connections	ault Web Site Home	Actions						
		🔊 Explore						
Start Page Filter:	- 🤝 Go - 🔙 Show All Group by:	Edit Permissions						
		Edit Site						
A Sites		Bindings						
Default Web Sit		Basic Settings						
j Explore	.NET Error .NET .NET Profile	View Applications						
Edit Permissions	n Pages Globalization	View Virtual Directories						
Add Application		Manage Webrite						
Add Virtual Directo	ry 💷 🚺 🔳 📕							
	.NET Users Application Connection	Kestart						
Edit Bindings	Settings Strings	▶ Start						
Manage Website	• 兪 🕵 🔍	Stop						

Рисунок 7.36 – Переход к меню создания виртуальной директории

В открывшемся окне (рисунок 7.37) введите наименование в поле *Alias* и укажите путь для каталога в поле *Physical path*.

Add Virtual Directory ? ×
Site name: Default Web Site Path: /
<u>A</u> lias:
CRLD
Example: images
Physical path:
C:\CRLDist
Pass-through authentication
Connect as Test Settings
OK Cancel

Рисунок 7.37 – Создание виртуальной директории

После нажатия кнопки **ОК** перейдите в левой части окна к созданной виртуальной директории и откройте пункт **Directory Browsing** (рисунок 7.38).





Рисунок 7.38 – Переход к просмотру каталогов

В следующем окне (рисунок 7.39) в правой части меню окна, нажмите на кнопку *Enable* для включения просмотра каталогов.



Рисунок 7.39 – Включение просмотра каталогов

Перейдите в левой части окна к созданной виртуальной директории и откройте пункт *Configuration Editor* (рисунок 7.40).



8	Internet Information Services (IIS) Manager	_ D X				
SoyDC > Sites > Default Web Site > CRLD >						
<u>F</u> ile <u>V</u> iew <u>H</u> elp						
Connections Start Page S09DC (PKI\Administrator) Application Pools Sites ADPolicyProvider_CEP_Kert P	Filter: Image: Show All Group by: Machine Key Pages and Controls Providers Session State SMTP E-mail IS Image: Show All Group by: Authentic Compression Default Default Document Default Document Directory Browsing Failed Handler Handler Failed Handler HTTP Request Tra Mappings Image: Show All Group by: MIME Types Modules Management Image: Show All Group by: Image: Controls Image: Show All Controls Image: Controls Image: Sho	Actions Open Feature Explore Edit Permissions Basic Settings Manage Virtual Directory Browse Virtual Directory Browse *:80 (http) Browse *:443 (https) Edit Virtual Directory Advanced Settings Image: Help				
Keady	Features View 🕂 Content View	•				

Рисунок 7.40 – Переход к редактору конфигураций

В открывшемся окне (рисунок 7.41) в поле **Section** выберите в раскрывающемся списке **system.webServer** \rightarrow **security** \rightarrow **requestFiltering**.



Рисунок 7.41 – Выбор раздела редактора конфигураций

Для параметра *allowDoubleEscaping* установите значение *True* (рисунок 7.42) и нажмите кнопку *Apply* в правой части окна.



8	Internet Info	rmation Services (IIS) Manager		_ D X
€ S09DC → Sites	Default Web Site CRLD			🕶 🛛 🏠 🔞 🕶
<u>F</u> ile <u>V</u> iew <u>H</u> elp				
Connections Image: Image Image: Image Image: Image	Configuration Edito Section: system.webServer/security/req	uestF From: Default Web Site/CRLD Web.config		Actions Apply Cancel
Application Pools	Deepest Path: MACHINE/WEBROOT/APPHOST			denerate Script
⊿ 🔞 Sites	allowDoubleEscaping	True	~	Configuration
⊿ 😔 Default Web Site	allowHighBitCharacters	True		Search Configuration
ADPolicyProvider_	alwaysAllowedQueryStrings	(Count=0)		Section 🔿
aspnet_client	alwaysAllowedUrls	(Count=0)		Lock Section
D CRLD	denyQueryStringSequences	(Count=0)		LOCK SECTION
b 👘 ocsp	denyUrlSequences	(Count=0)		'allowDoubleEscaping'
▷ ·· 🔐 pki-S09DC-CA_CES	b fileExtensions			Attribute
	filteringRules	(Count=0)		Lock Attribute
	b hiddenSegments			A Halp
	requestLimits			The second secon
	unescapeQueryString	True		
	▷ verbs			

Рисунок 7.42 – Настройка раздела редактора конфигураций

Перейдите к созданному каталогу (рисунок 7.43), в котором будут размещены списки отзывов (в примере *C:\CRLDist*) и откройте свойства каталога по щелчку правой кнопки мыши на каталоге.

📇 I 💽 🚯 👳 I		Local Disk (C:)			_ D X
File Home Share	View				~ ?
🔄 🏵 👻 🕆 👗 🕨 Th	nis PC 🔸 Local Disk (C:) 🔸		~	C Search Local D	isk (C:) 🔎
🔆 Favorites	Name	Da	ate modified	Туре	Size
🗾 Desktop	퉬 BlockHost	16	5.03.2021 16:01	File folder	
🗼 Downloads	퉬 CRLDist 📃	15	06.2023.8.56	File folder	
📃 Recent places	퉬 inetpub	Open	6	File folder	
	PerfLogs	Open in new window	2	File folder	
🌉 This PC	🌗 Program Files	Share with	▶ 3	File folder	
膧 Desktop	🌗 Program Files (x86	Restore previous versio	ns 1	File folder	
Documents	🐌 Tmp	Include in library	۶ ا	File folder	
🐌 Downloads	🌗 token	Pin to Start	4	File folder	
🚺 Music	🐌 Users	Sand to	9	File folder	
📔 Pictures	Windows	Send to	3	File folder	
📴 Videos	Values	Cut	6	Text Document	1 KB
📥 Local Disk (C:)		Сору			
		Create shortcut			
📬 Network		Delete			
		Rename			
		Properties			

Рисунок 7.43 – Переход в свойства каталога

Перейдите во вкладку *Sharing* (рисунок 7.44) и нажмите кнопку *Advanced Sharing* для предоставления общего доступа к директории.



1		CRLD	ist Properties		x
General	Sharing	Security	Previous Versions	Customize	
Netwo	ork File and	l Folder Sh	aring		
	CRLDi Not Sh	st nared			
<u>N</u> etwo Not S	ork Path: Shared				
<u>S</u>	hare				
Advar Set ci advar	nced Sharir ustom perm nced sharir A <u>d</u> vanced	ng nissions, cr ng options. d Sharing	eate multiple shares	, and set other	
		0	K Cance	el <u>A</u> pp	ły

Рисунок 7.44 – Вкладка Sharing

В появившемся окне установите флаг *Share this folder*, в поле *Share name* укажите «*CRLDist*\$» (рисунок 7.45).

Advanced Sharing ×
✓ Share this folder
Settings
S <u>h</u> are name:
CRLDist\$
Add Remove
Limit the number of simultaneous users to:
Comments:
Permissions Caching
OK Cancel Apply

Рисунок 7.45 – Установка расширенного доступа

Нажмите на кнопку *Permissions* (рисунок 7.46) и в появившемся окне нажмите Add для



предоставления разрешений контроллеру домена (рисунок 7.47).

Permissions	for CRLDist\$	x
Share Permissions		
Group or user names:		
Sector Everyone		
		- 1
	A <u>d</u> d <u>R</u> emove	
Permissions for Everyone	Allow Deny	_
Full Control		
Read		
- House	¥ L	
ОК	Cancel Apply	/

Рисунок 7.46 – Установка разрешений

Select Users, Computers, Service Accounts, or	Groups X
<u>S</u> elect this object type: Users, Groups, or Built-in security principals	Object Types
From this location:	
pki.local	Locations
Enter the object names to select (<u>examples</u>):	
1	Check Names
Advanced OK	Cancel

Рисунок 7.47 – Выбор типа для установки разрешений

По кнопке *Object types* (рисунок 7.48) установите флаг *Computers* и в поле *Enter the object names to select* введите имя контроллера домена (рисунок 7.49).



Object Types	x
Select the types of objects you want to find. Object types: Service Accounts Computers Groups Users Users	
OK Cano	el

Рисунок 7.48 – Выбор типа Компьютеры

Select Users, Computers, Service Accounts,	or Groups 🛛 🗙
<u>S</u> elect this object type: Users, Computers, Groups, or Built-in security principals	Object Types
From this location:	_
pki.local	Locations
Enter the object names to select (<u>examples</u>):	
S09DC	Check Names
Advanced OK	Cancel

Рисунок 7.49 – Выбор контроллера домена

Установите полный доступ для контроллера домена (рисунок 7.50).



Permissions for CRLDist\$	x
Share Permissions	
Group or user names:	
S09DC (PKI\S09DC\$)	
A <u>d</u> d <u>R</u> emove	
Permissions for S09DC Allow Deny	_
Full Control	
Read	
OK Cancel Appl	у

Рисунок 7.50 – Установка разрешений для контроллера домена

Перейдите во вкладку **Security** (рисунок 7.51) и нажмите кнопку **Edit** для добавления в разрешения контролера домена.

👢 CRLDist Properties 🗙
General Sharing Security Previous Versions Customize
Object name: C:\CRLDist
<u>G</u> roup or user names:
& CREATOR OWNER
& SYSTEM
& Administrators (PKI\Administrators)
& Users (PKI\Users)
To change permissions, click Edit.
Permissions for CREATOR
OWNER Allow Deny
Full control
Modify
Read & execute
List folder contents
Read
Write 🗸
For special permissions or advanced settings, Advanced Advanced.
OK Cancel Apply

Рисунок 7.51 – Вкладка **Security**



В появившемся окне нажмите *Add* для предоставления разрешений контроллеру домена (рисунок 7.52).

Permissions	for CRLDist	x
Security		
Object name: C:\CRLDist		
Group or user names:		
CREATOR OWNER		
Administrators (PKI\Administra & Users (PKI\Users)	ators)	
	A <u>d</u> d <u>R</u> emove	
Permissions for CREATOR OWNER	Allow Deny	
Full control		<u>~</u>
Modify		_
Read & execute		=
List folder contents		
Read		\neg
ОК	Cancel Apply	/

Рисунок 7.52 – Установка разрешений

По кнопке *Object types* (рисунок 7.48) установите флаг *Computers* и в поле *Enter the object names to select* введите имя контроллера домена (рисунок 7.49).

Установите полный доступ для контроллера домена (рисунок 7.53).



Permissions	for CRLDist	x
Security		
Object name: C:\CRLDist		
Group or user names:		
& CREATOR OWNER		
SYSTEM		
Administrators (PKI\Administr	ators)	
SUBUC (PKI\SUBUC\$)		
	A <u>d</u> d	<u>R</u> emove
Permissions for S09DC	Allow	Deny
Full control	✓	
Modify		
Read & execute	✓	
List folder contents	✓	
Read	✓	
		A 1
OK	Cancel	Арріу

Рисунок 7.53 – Установка разрешений для контроллера домена

7.7.3 Публикация списка отзывов

Перейдите к настройкам центра сертификации и откройте оснастку *Certification Authority* (рисунок 7.21).

В левой части окна перейдите в пункт *Revoked Certificates* и по щелчку правой кнопки мыши выберите *All Tasks* → *Publish* для публикации списка отзывов (рисунок 7.54).

📮 certsrv - [Cer	rtification Au	ithority (Local)\p	ki-S09DC-CA\Revoked	Certificates]	
File Action View Help Image: Constraint of the second seco					
Certification Authority (Local) Certification Authority (Local) Pki-S09DC-CA Revoked Certificate Susued Certific All Tas Pending Requ Failed Reques Certificate Ter Export Proper Holp	Request ID 9 iks h List ties	Revocation Date 11.11.2020 16:53 10.11.2020 14:53 Publish	Effective Revocation Date 30.11.1999 3:00 0.11.1999 3:00 0.11.1999 3:00	Revocation Reason Unspecified Unspecified Unspecified	Requester f PKI\Admin PKI\Admin PKI\Admin

Рисунок 7.54 – Переход к публикации списка отзывов

В появившемся окне выберите тип публикации New CRL и нажмите OK (рисунок 7.55).

Publish CRL	x
The latest published Certificate Revocation List (CRL) is still valid. Clients may not receive a new CRL until after their current one expires.	
Type of CRL to publish: New CRL Issues a complete CRL, which contains up to date revocation information for the CA. 	
◯ <u>D</u> elta CRL only	
Issues an abbreviated version of the CRL, which contains only the updates to the CRL that have been made since the last time it was published.	
OK Cancel	

Рисунок 7.55 – Публикация нового списка отзывов

В результате в выбранной директории будут опубликованы списки отзывов (рисунок 7.56).

🌆 l 💽 📓 = l	CF	RLDist		_ D X
File Home Share	View			~ ()
🔄 🍥 👻 🕈 퉬 🕨 Th	is PC → Local Disk (C:) → CRLDist	~ (Search CRLDist	م ر
🔆 Favorites	Name	Date modified	Туре	Size
📃 Desktop	🗵 pki-S09DC-CA	15.06.2023 11:28	Certificate Revoca	1 KB
〕 Downloads	E pki-S09DC-CA+	15.06.2023 11:28	Certificate Revoca	1 KB
🕮 Recent places	web.config	15.06.2023 11:24	CONFIG File	1 KB
This PC Desktop Documents Downloads Music Pictures Videos Local Disk (C:)				

Рисунок 7.56 – Опубликованный список отзывов сертификатов

7.8 Настройка подключения к домену из консоли управления по протоколу *Idaps* с установкой ssl-сертификатов

Подключение к домену из консоли управления СЗИ от НСД «Блокхост-Сеть 4» может осуществляться:

- **без пароля** – подключение по протоколу *Idap* с использованием билета *kerberos* (используется механизм *gssapi*);

по имени пользователя и паролю – подключение по протоколу Idaps, который



обеспечивает безопасность передачи пароля пользователя при подключении (подключение по *Idaps* выполняется с установкой ssl-сертификатов и требует дополнительных настроек).

7.8.1 Настройка контроллера домена AD

Для подключения к домену AD по протоколу *ldaps* с установкой ssl-сертификатов на рабочей станции с ролью центра сертификации (Certification Authority) запустите консоль центра сертификации с помощью команды *certsrv.msc* в командной строке (рисунок 7.57).



Рисунок 7.57 – Запуск консоли центра сертификации

В левой части окна перейдите на пункт Шаблоны сертификатов (Certificate Templates), щелкните правой кнопкой мыши и выберите Управление (Manage) (рисунок 7.58).

ها ا			certsrv - [0	Certification Authority (Local)\diff-S18CA02-CA\Certificate Templates]	_ 0 ×
File Action View	Help				
(• • (a) 🙆	2				
Certification Authori	ty (Local)	Name	•	Intended Purpose	
a diff-S18CA02-CA		Administ	rator	Microsoft Trust List Signing, Encrypting	
Revoked Cert	ificates	Basic EFS		Encrypting File System	
Issued Certific	cates	Compute	er	Client Authentication, Server Authentic	
Pending Requ	uests	Copy of	Enrollment Agent	Certificate Request Agent	
Failed Reques	sts	Directory	Email Replication	Directory Service Email Replication	
Certificate Te	Mar	nage	ntroller	Client Authentication, Server Authentic	
			ntroller Authentication	Client Authentication, Server Authentic	
	New	v	y Agent	File Recovery	
	View	v	 Agent 	Certificate Request Agent	
	Refr	resh	Agent 4 Different	Certificate Request Agent	
	5.m	and then	r true	Smart Card Logon, Client Authenticatio	
	Expe	DIT LISL.	thentication	Client Authentication, Server Authentic	
	Help	P	thentication with ViPNet	KDC Authentication, Smart Card Logon	
		🗟 One Day	Smartcard Logon RSA	Client Authentication, Smart Card Logon	
		PKI Com	puter	Server Authentication, Client Authentic	
		PKI Enrol	Iment Agent (Computer)	Certificate Request Agent	
		PKI Smar	tcard User (EA)	Smart Card Logon, Client Authenticatio	
		PKI Web	Server	Server Authentication	
		Smartcar	d Logon RSA	Smart Card Logon, Client Authentication	
		Smartcar	d Logon RSA 2	Client Authentication, Smart Card Logon	
		Smartcar	d Logon RSA 234	Smart Card Logon, Client Authentication	
		Smartcar	d Logon ViPNet	Smart Card Logon, Client Authentication	

Рисунок 7.58 – Управление шаблонами сертификатов

В появившемся окне выберите пункт *Kerberos Authentication* (рисунок 7.59).

Для создания копии имеющегося шаблона, щелкните правой кнопкой мыши и выберите *Скопировать шаблон (Duplicate Template)* (рисунок 7.59).

.	Cer	tificate Te	mplates Console			_ D X
File Action View Help						
⇐ ➡ 🖬 🖬 🗟 🖬						
ertificate Templates (s09dc.pki.local)	Template Display Name		Schema Version	Versi	In ^	Actions
	🚇 Domain Controller		1	4.1		Certificate Templates (s09dc 🔺
	🛛 🗵 Domain Controller Authentica	tion	2	110.0	С	Mars A diana
	🚇 EFS Recovery Agent		1	6.1		More Actions •
	🖳 🖳 Enrollment Agent		1	4.1		Kerberos Authentication
	🖳 🖳 Enrollment Agent (Computer)		1	5.1		More Actions
	🖳 🖳 Enrollment Agent CA		2	100.3	C	
	🖳 🖳 Enrollment Agent token syster	n	2	100.5	C—	
	🖳 🚇 Exchange Enrollment Agent (C	Offline requ	1	4.1		
	🖳 🖳 Exchange Signature Only		1	6.1		
	Exchange User		1	7.1		
	IPSec		1	8.1		
	IPSec (Offline request)		1	7.1		
	Rerberos Authentication	Durlinet	• Temendate	110.0	С	
	🖳 🖳 Key Recovery Agent	Duplicati	e i empiate	5.0	Ki	
	Response Signing	Reenroll	All Certificate Holders	1.0	0	
	RAS and IAS Server	All Tasks	;	1.0	С	
	Root Certification Authority	Properti	ec		≡	
	Router (Offline request)	Tropera				
	Smartcard Logon	Help				
	Smartcard Logon CA		2	100.5	Sr	
	🛛 🕮 Smartcard Logon Token syster	m	2	100.8	Sr	
	🖳 🕮 Smartcard User		1	11.1		
	Subordinate Certification Auth	nority	1	5.1		
	🛛 🚇 Trust List Signing		1	3.1		

Рисунок 7.59 – Создание копии шаблона

В появившемся окне со свойствами шаблона выполните следующие настройки:

1) Введите имя создаваемого шаблона на вкладке *Общие (General)*. Например, LDAPoverSSL. При необходимости настройте *Срок действия сертификата (Validity period)* и *Период обновления (Renewal period)* и опубликуйте его в AD *(Publish certificate in Active Directory)* (рисунок 7.60).



Pro	perties of	New Temp	late	×
Subject Name	Server	Issu	iance Re	equirements
Superseded Temp	ates	Extensions		Security
Compatibility General	Request Har	ndling Cryptog	graphy	Key Attestation
Template display name	e			
LDAPoverSSL				
Template name: LDAPoverSSL				
Validity period:	F	enewal period: 6 weeks	~	
✓ Publish certificate in □ Do not automat Directory	n Active Direct	ory a duplicate cert	tificate e	xists in Active
ОК	Can	cel A	pply	Help

Рисунок 7.60 – Свойства шаблона, вкладка General

2) Во вкладке **Обработчик запросов (Request Handling)** установите параметр **Разрешить экспорт закрытых ключей (Allow private key to be exported)** и нажмите **ОК** для сохранения шаблона (рисунок 7.61).



	Prope	erties	of New	Template		ĸ		
Subject Nam	e	Sen	ver	Issuance Requirements				
Superseded	Template	s	Exte	nsions	Security			
Compatibility Ge	eneral F	Request	Handling	Cryptography	Key Attestation			
<u>P</u> urpose:	Signatu	re and e	ncryption		~			
Delete revoked or expired certificates (do not archive)								
	Include symmetric algorithms allowed by the subject							
	Archive subject's encryption private key							
Authori <u>z</u> e ad	ditional se sions	ervice ad	counts to a	access the priva	ate key (*)			
✓ Allow private	key to be	e exporte	ed					
Renew with	the same	key (*)						
Eor automation new key can	c renewal inot be cr	l of smar eated ("	t card certil)	icates, use the	existing key if a			
Do the following associated with	when the this certifi	e subjec icate is u	t is enrolled used:	and when the	private key			
Enroll subject	t without	requiring) any user i	nput				
O Prompt the u	ser during	g enrollm	ent					
O Prompt the up private key is	ser during s used	g enrollm	ent and red	quire user input	when the			
* Control is disat	oled due t	o <u>compa</u>	atibility setti	ngs.				
	ОК	(Cancel	Apply	Help			

Рисунок 7.61 – Свойства шаблона, вкладка *Request Handling*

Для публикации созданного шаблона, после его настройки, перейдите на пункт *Шаблоны сертификатов (Certificate Templates)*, щелкните правой кнопкой мыши и выберите *Создать (New)* → *Выдаваемый шаблон сертификата (Certificate Template to Issue)* (рисунок 7.62).

i a	certsrv - [Certi	ficatio	n Authority (Local)\diff-S18C	A02-C/	A\Certificate Templates]	□ X
File Action V	/iew Help					
(* 🔿 🖄	1 🗟 👔					
違 Certification A	uthority (Local)	Name		Intende	ed Purpose	^
⊿ 👼 diff-S18CA	02-CA	🖳 CA	Exchange	Private	Key Archival	
🚞 Revoke	ed Certificates	🗷 Sm	artcard Logon RSA 3	Client	Authentication, Smart Card Logon	
📔 Issued	Certificates	🖳 Sm	artcard Logon RSA 234	Smart	Card Logon, Client Authentication	
📔 Pendin	g Requests	🗷 Sm	artcard Logon RSA 2	Client	Authentication, Smart Card Logon	
Failed F	Requests	🖳 JM	S operator true	Smart	Card Logon, Client Authenticatio	
Certific	ate Templates		Day Smartcard Logon RSA	Client	Authentication, Smart Card Logon	
	Manage		Allment Agent	Certific	ate Request Agent	
	New	•	Certificate Template to Issue		ite Request Agent	=
	View	+	Computer	Server	Authentication, Client Authentic	
	Defeet		Web Server	Server	Authentication	
	Refresh		Smartcard User (EA)	Smart	Card Logon, Client Authenticatio	
	Export List		Ilment Agent 4 Different	Certific	ate Request Agent	
	Help		irtcard Logon ViPNet	Smart	Card Logon, Client Authentication	
		😬 Sm	artcard Logon RSA	Smart	Card Logon, Client Authentication	
		🖳 Ke	beros Authentication with ViPNet	KDC A	uthentication, Smart Card Logon	
		🖳 Dir	ectory Email Replication	Directo	ory Service Email Replication	
		🗷 Do	main Controller Authentication	Client	Authentication, Server Authentic	
		🗷 Kei	beros Authentication	Client	Authentication, Server Authentic	
		🖳 EFS	Recovery Agent	File Re	covery	
		🗷 Bas	sic EFS	Encryp	ting File System	
		🗷 Do	main Controller	Client	Authentication, Server Authentic	~
Enable additional (Certificate Template	s on this	Certification Authority			

Рисунок 7.62 – Выбор выдаваемого шаблона сертификата

В появившемся окне (рисунок 7.63) выберите созданный шаблон сертификата и нажмите **ОК**.

En En	able Certificate Templates	3
Select one Certificate Template to enable Note: If a certificate template that was rece information about this template has been re All of the certificate templates in the organi For more information, see <u>Certificate</u>	on this Certification Authority. ently created does not appear on this list, you may need to wait until eplicated to all domain controllers. zation may not be available to your CA. <u>Template Concepts.</u>	
Name	Intended Purpose	
IPSec	IP security IKE intermediate	
IPSec (Offline request)	IP security IKE intermediate	
Rey Recovery Agent	Key Recovery Agent	
Real LDAPoverSSL	KDC Authentication, Smart Card Logon, Server Authentication	
OCSP Response Signing	OCSP Signing	
RAS and IAS Server	Client Authentication, Server Authentication	≡
Router (Offline request)	Client Authentication	
🚇 Smartcard Logon	Client Authentication, Smart Card Logon	
🚇 Smartcard User	Secure Email, Client Authentication, Smart Card Logon	\square
R Trust List Signing	Microsoft Trust List Signing	\mathbf{M}
<	III >	
	OK Cance	<u>+</u>

Рисунок 7.63 – Публикация созданного шаблона

На контроллере домена, для которого планируется задействовать LDAPS, необходимо



наличие в оснастке *Сертификаты (Certificates)* в разделе *Личные (Personal)* установленного сертификата, выпущенного по шаблону созданного сертификата.

Для создания сертификата выполните следующие действия:

1) Перейдите в оснастку сертификатов *certmgr.msc* (рисунок 7.64).



Рисунок 7.64 – Оснастка Сертификаты (Certificates)

2) В левой части окна перейдите в раздел *Личные (Personal)* и по щелчку правой кнопкой мыши выберите *Все задачи (All Task)* → *Запросить новый сертификат (Request New Certificate)* (рисунок 7.65).



🔤 certmgr - [Сертификаты - текущий пользов	атель\Личное]		
Файл Действие Вид Избранное О	кно Справка	1	- 8 ×
Сертификаты - текущий пользователь		Тип объекта	
Поиск сертификатов	ации	Сертификаты	
Все задачи	Поиско	сертификатов	
🕨 🧧 Вид 🔸	Запрос	ить новый сертификат	
Новое окно отсюда	Импорт	Tow	
Новый вид панели задач	Дополн	ительные операции	
 Обновить Экспортировать список 	рт-карты		
Справка			
	-		
Запросить новый сертификат от центра сертис	ф <mark>икации (ЦС) в</mark>	этом домене	

Рисунок 7.65 – Запрос нового личного сертификата

3) В появившемся окне *Регистрация сертификатов* выберите *Политика регистрации Active Directory (Active Directory Enrollment Policy)* и нажмите *Далее* (рисунок 7.66).

Регистрация сертификатов	
Выбор политики регистрации сертификатов	
Политика регистрации сертификатов позволяет регистрировать сертиф заранее шаблонов сертификатов. Политика регистрации сертификатов	рикаты на основании заданных уже могла быть настроена.
Настраиваемые администратором	
Политика perистрации Active Directory	•
Настраиваемые пользователем	Добавить
Дополнительные сведения о <u>политике регистрации сертификатов</u>	
	Далее Отмена

Рисунок 7.66 – Выбор политики регистрации сертификата

4) Выберите шаблон сертификата, созданный в центре сертификации (например, *LDAPoverSSL*) (рисунок 7.67).

Request Certificates		
You can request the following	types of certificates. Select the certificates you want to request, and the	'n
click Enroll.		
LDAPoverSSL	i) STATUS: Available Details	~ _
The following options de	scribe the uses and validity period that apply to this type of certificate:	
Key usage:	Digital signature	
	Key encipherment	
Application policies:	KDC Authentication	
	Smart Card Logon	
	Client Authentication	
Validity period (days)	730	
renary period (doys).	Droportion	
	Properties	

Рисунок 7.67 – Выбор шаблона сертификата

5) Дождитесь выпуска и установки сертификата в хранилище **Личное** и нажмите **Готово**.

Для взаимодействия контроллера домена и рабочей станции с установленной консолью управления через *LDAPS* необходимо установить доверие удостоверяющему центру (CA), который выдал сертификат для контроллера домена:

1) На рабочей станции с ролью центра сертификации (Certification Authority) выполните экспорт корневого сертификата удостоверяющего центра в файл с помощью команды:

```
certutil -ca.cert ca_name.cer
```

Файл сертификата сохранится в профиле текущего пользователя с именем *ca_name.cer*.

2) Добавьте экспортированный сертификат в хранилище сертификатов **Trusted Root Certification Authorities** на рабочей станции с установленной консолью управления и контроллере домена вручную через оснастку управления сертификатами или из командной строки:

certutil -addstore -f "ROOT" <path_to_certificate>

3) Перезапустите службы Active Directory на контроллере домена, либо перезагрузите контроллер домена.

7.8.2 Настройка контроллера домена Samba

Для подключения к домену Samba по протоколу *ldaps* с установкой ssl-сертификатов установите пакет **openssl**.

На контроллере домена, для которого планируется задействовать *ldaps* выполните генерацию корневой пары ключ-сертификат:

```
openssl genrsa -out rootCA.key 2048
openssl req -x509 -new -key rootCA.key -days 10000 -out rootCA.crt
```

Выполните генерацию приватного ключа и сертификата, подписанного корневым сертификатом:

openssl genrsa -out lnx-dc11.alt.test.key 2048
openssl req -new -key lnx-dc11.alt.test.key -out lnx-dc11.alt.test.csr

Ответьте на вопросы.

 (\mathbf{i})

При ответах на вопросы важно учитывать следующее:

1) в поле *Common Name* важно указать FQDN имя хоста, для которого генерируется сертификат;

2) можно заполнить только поле Common Name;

3) ответы на вопросы для первого или второго сертификата <u>не должны</u> <u>совпадать,</u> иначе рабочая станция с установленной консолью управления считает такой сертификат невалидным (самоподписанным) и подключение не удастся.

При подключении к домену с проверкой сертификатов, подключение будет успешно, когда подключение осуществляется по имени, указанному в поле **Соттоп пате** или в поле **Дополнительное имя субъекта** (рисунок 7.68).



🙀 Сертификат	🗙 🛃 Сертификат 🛛 🗙
Общие Состав Путь сертификации	Общие Состав Путь сертификации
Показать: <bce> Поле Значение Ф. Идентификатор ключа су 9bc4ee93e9bca3d34ef755d5 Ф. Идентификатор ключа су 9bc4ee93e9bca3d34ef755d5 Ф. Идентификатор ключа су 9bc4ee93e9bca3d34ef755d5 Ф. Идентификатор ключа су 11/очка распределения сти Ф. Доступ к информации о це [1]Лочка распределения сти Ф. Доступ к информации о це [1]Доступ к сведениян цент Ф. Использование ключа Цифровая подпись, Шифров Ф. Отпечаток 2637879b7002a7a30e023119</bce>	Показать: <a>Все> Поле Эначение Субъект Субъект Параметры открытого кл Открытый ключ Параметры открытого кл 05 00 Идентификатор ключа су Очовные ограничения Основные ограничения Основные ограничения Оспечаток У
Свойства Копировать в файл	іл Свойства Копировать в файл
OF	ОК

Рисунок 7.68 – Подключение по имени в поле Дополнительное имя субъекта

B openssl поле Дополнительное имя субъекта по умолчанию не задается, для его включения следует обратиться к дополнительным инструкциям, например, https://r-notes.ru/administrirovanie/poleznosti/164-openssl-sozdaniemultidomennogo-sertifikata.html.

openssl x509 -req -in lnx-dc11.alt.test.csr -CA rootCA.crt -CAkey rootCA.key -CAcreateserial
-out lnx-dc11.alt.test.crt -days 5000

В итоге получаем комплект:

Cert: lnx-dc11.alt.test.crt
Key: lnx-dc11.alt.test.key
CA: rootCA.crt

Выполните настройку SSL/TLS на контроллере домена Samba:

1) Сгенерированные ключи скопируйте в рабочий каталог Samba (от имени суперпользователя):

```
# cp lnx-dc11.alt.test.crt /var/lib/samba/private/tls/
# cp lnx-dc11.alt.test.key /var/lib/samba/private/tls/
# cp rootCA.crt /var/lib/samba/private/tls/
```

2) В секцию *Global* в /*etc/samba/smb.conf* добавьте следующие параметры:

```
ldap server require strong auth = yes
tls enabled = yes
tls keyfile = tls/lnx-dc11.alt.test.key
```

tls certfile = tls/lnx-dc11.alt.test.crt

3) Перезапустите сервис Samba:

systemctl restart samba

7.8.3 Настройка контроллера домена FreeIPA

Для подключения к домену FreeIPA по протоколу *ldaps* с установкой ssl-сертификатов нет необходимости устанавливать сертификаты, т.к. они уже присутствуют на домене FreeIPA.

Для выполнения настройки подключения к домену FreeIPA требуется только экспортировать цепочку корневых сертификатов с сервера и установить их на рабочие станции с установленной консолью управления.

7.8.4 Настройки на рабочей станции OC Windows с установленной консолью управления

Для подключения к домену по протоколу *ldaps* с установкой ssl-сертификатов необходимо на рабочей станции под управлением OC Windows с установленной консолью управления выполнить следующие действия:

1) Экспортировать корневой сертификат удостоверяющего центра на рабочую станцию.

2) Добавить корневой сертификат в хранилище сертификатов **Trusted Root Certification Authorities** вручную через оснастку управления сертификатами или из командной строки:

certutil -addstore -f "ROOT" <path_to_certificate>

где *<path_to_certificate>* - путь к файлу с экспортированным корневым сертификатом.

3) Для добавления цепочки корневых сертификатов повторите приведенные действия для всех сертификатов цепочки.

7.8.5 Настройки на рабочей станции ОС Linux с установленной консолью управления

Подключение к домену по протоколу *ldaps* с установкой ssl-сертификатов на рабочей станции под управлением OC Linux с установленной консолью управления возможно несколькими способами:

Вариант 1 (рекомендуемый):

При необходимости выполните преобразование файла в формате .*cer* в файл в формате .*crt* с помощью команды:

openssl x509 -inform der -in certificate.cer -out certificate.crt

где certificate.cer – файл в формате .cer, certificate.crt – файл в формате .crt.

В конфигурационном файле *Idap* (путь к файлу */etc/openIdap/Idap.conf* в ОС Альт, РЕД ОС или */etc/Idap/Idap.conf* в ОС AstraLinux) на рабочей станции под управлением ОС Linux с установленной консолью управления задайте параметр *TLS_CACERT* и укажите путь к файлу, в котором приведены все необходимые сертификаты:

TLS_CACERT /etc/ssl/certs/ca-certificates.crt

i

Файл *ca-certificates.crt* может содержать несколько сертификатов, каждый из которых начинается с -----*BEGIN CERTIFICATE*----- и заканчивается на -----*END CERTIFICATE*-----. Администратору нужно добавить в файл все необходимые сертификаты для организации безопасного подключения.

Для добавления цепочки корневых сертификатов повторите приведенные действия для всех сертификатов цепочки.



Если параметр TLS_CACERT задан, то сертификаты, добавленные другими способами, будут проигнорированы при подключении.

<u>Вариант 2:</u>

Для добавления корневого сертификата необходимо выполнить следующие шаги:

1) На рабочую станцию под управлением ОС Linux с установленной консолью управления экспортируйте необходимый корневой сертификат.

2) В терминале выполните команду

sudo trust anchor --store <path_to_certificate>

где *path_to_certificate* – путь к файлу с экспортируемым корневым сертификатом.

3) Нажмите *Enter* и введите пароль администратора, если потребуется.

4) Для добавления цепочки корневых сертификатов повторите приведенные действия для всех сертификатов цепочки.



Сертификаты, заданные таким образом, игнорируются, если в config-файле задан параметр *TLS_CACERT*.

<u>Вариант 3:</u>

Для добавления корневого сертификата необходимо выполнить следующие шаги:

1) На рабочую станцию под управлением OC Linux с установленной консолью управления в системный репозиторий сертификатов от имени суперпользователя добавьте корневой сертификат:

cp <path_to_certificate> /etc/pki/ca-trust/source/anchors/
update-ca-trust



2) Для добавления цепочки корневых сертификатов повторите приведенные действия для всех сертификатов цепочки.



Сертификаты, заданные таким образом, игнорируются, если в config-файле задан параметр *TLS_CACERT*.

7.8.6 Проверка работоспособности подключения

На рабочей станции под управлением <u>OC Linux</u> для проверки работоспособности подключения можно использовать следующую команду:

ldapsearch -h "<[полное] имя домена>" -Z -x -LLL -b "" -s base supportedSASLMechanisms -d0

параметр *Z* – устанавливает ssl-соединение;

параметр *d* со значением «0» определяет минимальный уровень отладки (уровень отладки регулируется значением от 0 до 3).



При правильно настроенных сертификатах команда выводит список поддерживаемых алгоритмов, в противном случае – ошибку.

Для успешного подключения должны выполняться следующие условия:

домен доступен и настроен в части работы с сертификатами;

сертификат установлен;

 - <[полное] имя домена> соответствует значению поля Common name установленного сертификата;

– в файле конфигурации отсутствует/закомментирован параметр TLS_CACERT.

На рабочей станции под управлением <u>OC Windows</u> для проверки работоспособности подключения можно использовать утилиту *ldp.exe*.

Для проверки в окне подключения к домену указывается домен, порт (636 для ldaps) и выбирается поддержка ssl.

7.8.7 Особенности при настройке AD для подключения по ldaps из OC AstraLinux 1.7

На сервере центра сертификации (Certification Authority) при выпуске сертификата может использоваться алгоритм <u>SHA1, считающийся устаревшим</u> (рисунок 7.69).

В OC AstraLinux версии 1.7 с настройками по умолчанию такой сертификат будет считаться ненадежным и подключение к AD по такому сертификату работать не будет.

🙀 Сертификат		×	😡 Сертификат	×
Общие Состав Путь сертиф	икации		Общие Состав Путь сертификации	
Показать: <8се>	~		Показать: <все>	~
Поле Версия Серийный номер Алгоритм подписи Узш-алгоритм подписи Издатель Действителен с Действителен по ПС объект	Значение V3 55000002а816b9cf5686391a sha1RSA sha1 pki-S09DC-CA, pki, local 23 июня 2023 г. 12:53:03 23 июня 2025 г. 13:03:03	<	Поле Значение Версия V3 Серийный номер 6439f28f366 Алгоритм подписи sha256RSA Хэш-алгоритм подписи sha256 Издатель dc.domain.te Действителен с 6 июля 2023 Действителен по 21 ноября 20 Субъект dc domain te	890a6ea845302f st, section, gis, s r. 13:28:45 50 r. 13:28:45 st section gis s
	Свойства Копировать в фай.	n	Свойства	Копировать в файл
	0	к		ОК

Рисунок 7.69 – Сертификат, использующий sha1 (слева) и sha256 (справа)

Просмотреть используемый сертификат можно командой:

openssl x509 -in certificate.crt -text -noout

где certificate.crt – файл сертификата.

Для изменения алгоритма SHA1 на SHA256 в центре сертификации Windows CA воспользуйтесь инструкцией *https://www.bulygin.su/2016/04/sha1-sha256-windows-ca.html* и выполните следующие действия:

1) На сервере с ролью CA (Certification Authority) проверьте текущий используемый алгоритм командой:

certutil -getreg ca\csp\CNGHashAlgorithm

Если результат выполнения команды SHA256, перейдите к шагу 4.

2) Если результат выполнения команды **SHA1**, для перенастройки центра сертификации на использование SHA256 необходимо выполнить команду:

certutil -setreg ca\csp\CNGHashAlgorithm SHA256

3) Перезапустите *Certificate Services* с помощью команды:

net stop CertSvc && net start CertSvc

4) Перевыпустите корневой сертификат:

certutil -renewCert ReuseKeys

5) Перезапустите службу *Certificate Services*:

net stop CertSvc && net start CertSvc

В результате указанных действий будет создан новый корневой сертификат центра сертификации с использованием SHA256 в качестве алгоритма подписи, который необходимо экспортировать на клиентские рабочие станции.



Перечень сокращений

CA	_	Certification Authority (удостоверяющий центр)
OU	_	Organizational Unit (организационное подразделение)
RSA	_	Аббревиатура от фамилий Rivest, Shamir и Adleman (криптографический алгоритм с открытым ключом)
НСД	_	Несанкционированный доступ
OC	_	Операционная система

СЗИ – Средство защиты информации