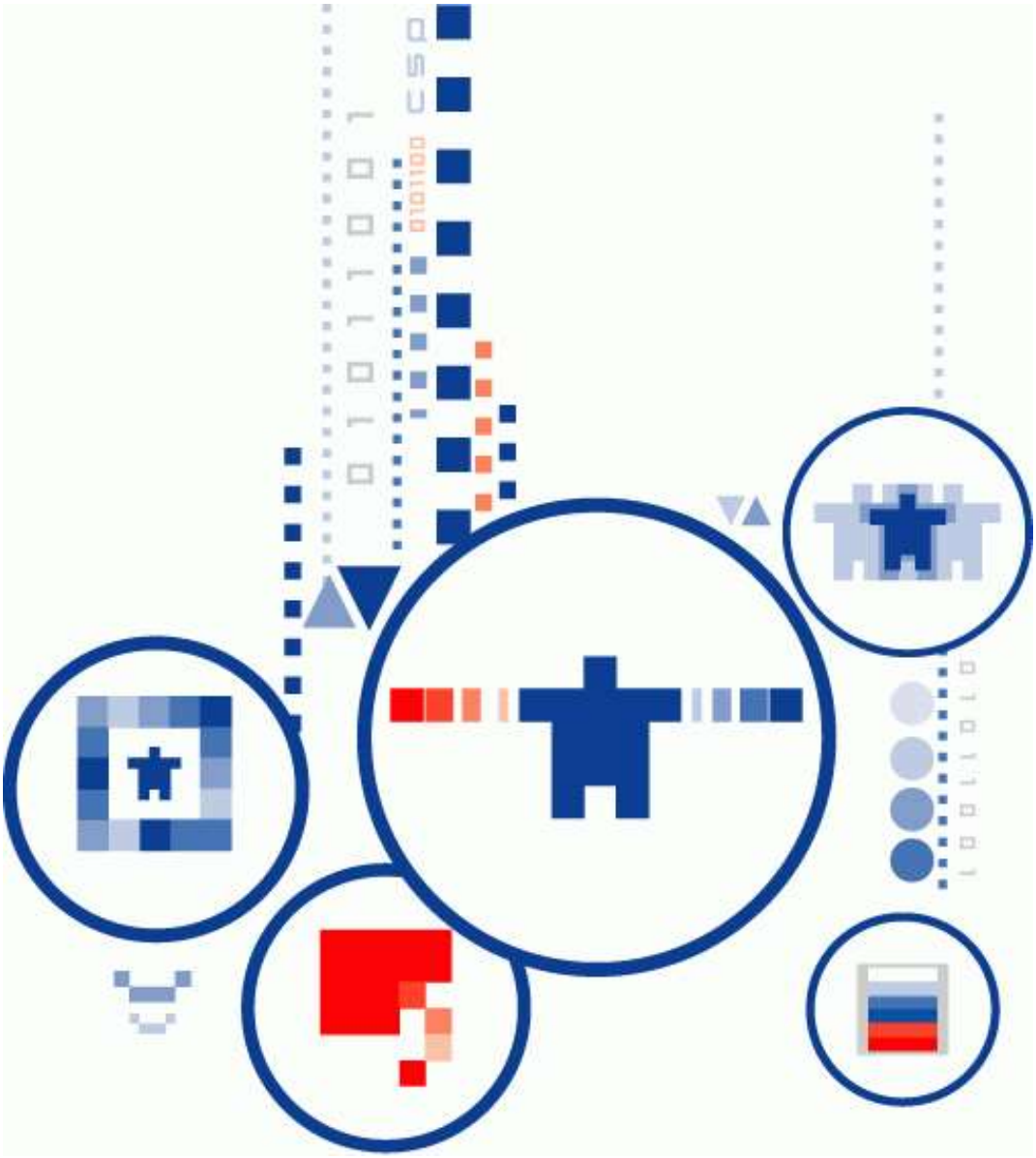

Модуль Автоматизированной Подписи для ПАК «КриптоПро DSS»

Версия 2.1

Руководство администратора

1. Описание Модуля Автоматизированной подписи

ПО Модуль автоматизированной подписи для ПАК «КриптоПро DSS» версии 2.1 (далее – «КриптоПро МАП», «МАП») предназначен для автоматизации процессов подписания PDF-документов электронной подписью с использованием Сервера Электронной Подписи «КриптоПро DSS».

2. Установка Модуля Автоматизированной Подписи

Для установки компонентов МАП служит самораспаковывающийся архив asm.exe.

3. Администрирование учётных записей

В дальнейшем предполагается, что все действия по разворачиванию МАП выполняются от имени пользователя «Администратор МАП» с правами администратора. Служба МАП выполняет действия от имени пользователя «Сервис МАП».

4. Конфигурация DSS

Для работы МАП необходимо произвести начальную конфигурацию DSS, включающую в себя создание OAuth клиента, создание оператора DSS, настройку аутентификации клиентов.

4.1. Создание OAuth клиента

Для возможности работы в DSS МАП должен быть зарегистрирован в качестве клиента DSS. Необходимо создать клиент с сценариями Implicit и ResourceOwner flow. Для регистрации используется командлет DSS Add-DssClient. Для более подробной информации о командлете – см. руководство администратора DSS. Пример регистрации клиента DSS:

```
Add-DssClient –Identifier AutoSigner –Name AutoSigner –AllowedFlow Implicit,
ResourceOwner, AuthorizationCode –RedirectUri urn:ietf:wg:oauth:2.0:oob:auto
```

Для активации аутентификации с использованием OAuth2 необходимо использовать командлет Enable-DssAuthenticationMethod:

```
Enable-DssAuthenticationMethod –Uri
http://dss.cryptopro.ru/identity/authenticationmethod/oath
```

4.2. Создание оператора DSS

Для осуществления действий МАП от имени пользователей DSS необходимо создать оператора DSS. Необходимо выпустить и установить сертификат Оператора DSS.

Для корректной работы МАП необходимо установить сертификат оператора в хранилище My\LocalMachine

Для создания используется командлет Add-DssIdentityOperator. Для более подробной информации о командлете – см. руководство администратора DSS. Пример регистрации оператора DSS:

```
Add-DSSIdentityOperator -Login DssOperator -Name DssOperator -IssuerName
realsts -Certificate c:\certs\operator.cer
```

4.3. Настройка аутентификации DSS

Для функционирования МАП необходимо задать на DSS возможность входа пользователей только по логину, а также разрешить использовать в качестве логина почту и номер телефона. Для этого используются командлеты DSS Set-DssStsProperties и Enable-DssAuthenticationMethod. Подробности в документации DSS.

Пример использования Set-DssStsProperties:

```
Set-DssStsProperties -AvailableIdentitifers Login,Email,PhoneNumber
```

Пример использования Enable-DssAuthenticationMethod:

```
Enable-DssAuthenticationMethod -Id 1
```

5. Конфигурация МАП

Настройка компонентов МАП состоит из следующих этапов:

- создание экземпляра МАП;
- конфигурация подключения к базе данных;
- конфигурация подключения к DSS;
- конфигурация подключения к LDAP;
- конфигурация подключения к WebSso;
- конфигурация параметров работы МАП;
- конфигурация ролей МАП;
- конфигурация веб интерфейса;
- создание начальных пользователей МАП;
- создание агента восстановления МАП.

5.1. Создание экземпляра МАП

Для создания экземпляра МАП служит командлет Add-AsmInstance.
Пример создания экземпляра МАП:

```
Add-AsmInstance
```

5.2. Конфигурация подключения к базе данных

Для работы с базой данных МАП необходимо предоставить доступ к базе данных учётным записям МАП. Для этого необходимо добавить пользователя «Администратор МАП» в роль «asmadministator» в базе данных «AutoSigner». Аналогично пользователя «Сервис МАП» в роль «asmserviceinstance».

Командлет Set-AsmDbConnection

Для конфигурации параметров подключения к существующей базе данных МАП используется командлет Set-AsmDbConnection.

Синтаксис:

```
Set-AsmDbConnection –ConnectionString <string>
```

Таблица 1. Параметры командлета Set-AsmDbConnection

Параметр	Требуется	Тип	Описание
ConnectionString	Нет	string	Задаваемая строка подключения к базе данных МАП.

Пример задания строки подключения:

```
Set-AsmDbConnection –ConnectionString "Data Source=WIN-SRV;Initial
Catalog=AutoSigner;Integrated Security=true;"
```

Командлет Get-AsmDbConnection

Для получения информации о текущей конфигурации используется командлет Get-AsmDbConnection.

Синтаксис:

```
Get-AsmDbConnection
```

5.3. Конфигурация подключения к DSS

Командлет Set-AsmDssConnection

Для задания параметров подключения к DSS используется командлет Set-AsmDssConnection.

Синтаксис:

```
Set-AsmDssConnection [-DssHostName <string>] [-SvsServiceAddress <string>] [-
SsAppName <string>] [-StsAppName <string>] [-OAuthClientId <string>] [-
AuthClientSecret <string>] [-OAuthRedirectUri <string>] [-OperatorCertificate
<X509Certificate>] [-ClientCertificate <X509Certificate>]
```

Таблица 2. Параметры командлета Set-AsmDssConnection

Параметр	Требуется	Тип	Описание
DssHostName	Нет	string	Url https адрес DSS

Параметр	Требуется	Тип	Описание
SvsServiceAddress	Нет	string	Url адрес SVS службы
SsAppName	Нет	string	Имя приложения сервиса подписи DSS
StsAppName	Нет	string	Имя приложения центра идентификации DSS
OAuthClientId	Нет	string	Идентификатор МАП как OAuth клиента DSS
OAuthClientSecret	Нет	string	Секрет МАП как OAuth клиента DSS. Для тестового пустой.
OAuthRedirectUri	Нет	string	OAuth RedirectUri
OperatorCertificate	Нет	X509Certificate	Сертификат аутентификации МАП, как оператора DSS
ClientCertificate	Нет	X509Certificate	Сертификат аутентфикации МАП, как клиента DSS

Для корректной работы МАП необходимо выдать права на закрытый ключи сертификатов оператора и клиента DSS для пользователя, «Сервис МАП». Сделать это можно через оснастку сертификаты.

Пример задания конфигурации подключения к DSS:

```
$operatorCert = Get-Item
"Cert:\LocalMachine\My\f1ccdb64217ba2f21eb2af7f2f391eea8f572720"
$clientCert = Get-Item
"Cert:\LocalMachine\My\d5db972526e7c9dcd760c262cc34b86c435c77fb"

Set-AsmDssConnection –DssHostName "https://dss.cryptopro.ru" -
SvsServiceAddress "http://dss-x64-w12r2/SVS/Service.svc" -SsAppName
"SignServer" -StsAppName "STS" -OAuthClientId "AutoSigner" -OAuthClientSecret
"" -OAuthRedirectUri "urn:ietf:wg:oauth:2.0:oob:auto" -OperatorCertificate
$operatorCert -clientCertificate $clientCert
```

Командлет Get-AsmDssConnection

Для отображения текущих параметров подключения к DSS используется командлет Get-AsmDssConnection.

Синтаксис:

```
Get-AsmDssConnection
```

5.4. Конфигурация подключения к LDAP

Командлет Set-AsmLdapConnection

Для подключения к LDAP используется командлет Set-AsmLdapConnection.

Синтаксис:

```
Set-AsmLdapConnection [-Address <string>] [-Port <int>] [-LdapUseSsl <bool>]
[-Credentials <PSCredential>] [-UserContainer<string>] [-
GroupContainer<string>]
```

Таблица 3. Параметры командлета Set-AsmLdapConnection

Параметр	Требуется	Тип	Описание
Address	Нет	string	Url адрес сервера LDAP
Port	Нет	int	Порт LDAP службы
LdapUseSsl	Нет	bool	Использовать SSL для подключения к LDAP
Credentials	Нет	PSCredential	Данные пользователя для подключения к LDAP
UserContainer	Нет	string	Имя контейнера пользователей
GroupContainer	Нет	string	Имя контейнера групп

Пример использования командлета Set-AsmDssConnection:

```
$secpasswd = ConvertTo-SecureString "PlainTextPassword" -AsPlainText -Force
$mycreds = New-Object System.Management.Automation.PSCredential("username",
$secpasswd)

Set-AsmLdapConnection -Address "ldap.db.com" -Port "84" -LdapUseSsl 0 -
UserContainer "cn=User" -GroupContainer "cn=group" –Credentials $mycreds
```

Командлет Get-AsmLdapConnection

Для отображения текущих параметров подключения к LDAP используется командлет Get-AsmLdapConnection.

Синтаксис:

```
Get-AsmLdapConnection
```

5.5. Конфигурация подключения к WebSso

Командлет Set-AsmWebSsoConnection

Для подключения к WebSso используется командлет Set-AsmWebSsoConnection.

Синтаксис:

```
Set-AsmWebSsoConnection [-Credentials <PSCredential>] [-LogoutUrl <string>]
[-WebSsoServiceAddress <string>]
```

Таблица 4. Параметры командлета Set-AsmWebSsoConnection

Параметр	Требуется	Тип	Описание
Credential	Нет	PSCredential	Данные пользователя для подключения к WebSso
LogoutUrl	Нет	string	Базовый URL выхода пользователя

Параметр	Требуется	Тип	Описание
WebSsoServiceAddress	Нет	string	Url службы WebSso

Пример использования командлета Set-AsmWebSsoConnection:

```
$secpasswd = ConvertTo-SecureString "PlainTextPassword" -AsPlainText -Force
$mycreds = New-Object System.Management.Automation.PSCredential("WebSsoAsm", $secpasswd)

Set-AsmWebSsoConnection -Credential $mycreds -LogoutUrl "https://login-intranet.isso.intranet.db.com/websso/sso_Logout.sso"
```

Командлет Get-AsmWebSsoConnection

Для отображения текущих параметров подключения к WebSso используется командлет Get-AsmWebSsoConnection.

Синтаксис:

```
Get-AsmWebSsoConnection
```

5.6. Конфигурация параметров работы МАП

Командлет Set-AsmProperties

Для конфигурации работы МАП используется командлет Set-AsmProperties.

Синтаксис:

```
Set-AsmProperties [-DbResponseTime <int>] [-UserSessionTimeOut <int>]
```

Таблица 5. Параметры командлета Set-AsmProperties

Параметр	Требуется	Тип	Описание
DbResponseTime	Нет	int	Период реагирования на изменения в базе данных в секундах
UserSessionTimeOut	Нет	int	Длительность пользовательской веб сессии в секундах
JobStopTimeOut	Нет	int	Таймаут ожидания остановки процессов в секундах
FileLockedTimeOut	Нет	int	Таймаут ожидания записи файлов в секундах

Пример использования командлета Set-AsmProperties:

```
Set-AsmProperties -DbResponseTime 120 -UserSessionTimeOut 600 -JobStopTimeOut 60 -FileLockedTimeOut 20
```

Командлет Get-AsmProperties

Для отображения текущей конфигурации МАП используется командлет Get-AsmProperties.

Синтаксис:

```
Get-AsmProperties
```

5.7. Конфигурация ролей МАП

Командлет Set-AsmRoleMapping

Для конфигурации ролей МАП используется командлет Set-AsmRoleMapping.

Синтаксис:

```
Set-AsmRoleMapping [-UserGroups <List<string>>] [-OperatorGroups <List<string>>]
[-AuditorGroups <List<string>>]
```

Таблица 6. Параметры командлета Set-AsmRoleMapping

Параметр	Требуется	Тип	Описание
UserGroups	Нет	List<string>	Список групп пользователей с ролью «Пользователь МАП»
OperatorGroups	Нет	List<string>	Список групп пользователей с ролью «Администратор МАП»
AuditorGroups	Нет	List<string>	Список групп пользователей с ролью «Аудитор МАП»

Пример использования командлета Set-AsmRoleMapping:

```
Set-AsmRoleMapping –UserGroups Users, Accountant –OperatorGroups AsmOperators
–AuditorGroup AsmAuditors
```

Командлет Get-AsmRoleMapping

Для отображения конфигурации ролей МАП используется командлет Get-AsmRoleMapping.

Синтаксис:

```
Get-AsmRoleMapping
```

5.8. Конфигурация веб интерфейса

Командлет Set-AsmFrontendProperties

Для конфигурации веб интерфейса МАП используется командлет Set-AsmFrontendProperties.

Синтаксис:

```
Set-AsmFrontendProperties [-ApiScheme <string>] [-ApiHost <string>] [-ApiPort
<int>] [-ApiPath <string>]
```

Таблица 7. Параметры командлета Set-AsmFrontendProperties

Параметр	Требуется	Тип	Описание
ApiScheme	Нет	string	Схема API МАП. Допустимые значения – "https", "http".
ApiHost	Нет	string	Адрес хоста API МАП
ApiPort	Нет	int	Порт API МАП
ApiPath	Нет	string	Относительный пусть к API МАП

Пример использования командлета Set-AsmFrontendProperties:

```
Set-AsmFrontendProperties -ApiScheme "https" –ApiHost "AsmDemo" –ApiPort "" –
ApiPath "/asm/api"
```

Командлет Get-AsmFrontendProperties

Для отображения конфигурации веб интерфейса МАП используется командлет Set- AsmFrontendProperties.

Синтаксис:

```
Get-AsmFrontendProperties
```

5.9. Создание начальных пользователей МАП

Для создания администраторов МАП используется командлет Add-AsmAdministrator.

Синтаксис:

```
Add-AsmAdministrator –Login <string>
```

Таблица 8. Параметры командлета Add-AsmAdministrator

Параметр	Требуется	Тип	Описание
Login	Да	string	Логин пользователя МАП. Должен состоять в группе советующей роли «Администраторы МАП»

Пример использования командлета Add-AsmAdministrator:

```
Add-AsmAdministrator –Login u_o_Prime@cryptopro.ru
Add-AsmAdministrator –Login u_o_Origin@cryptopro.ru
```

5.10. Создание агента восстановления МАП

Для создания агнета восстановления МАП используется командлет Set-AsmRecoveryAgent.

Синтаксис:

```
Set-AsmRecoveryAgent –Login <string>
```

Таблица 9. Параметры командлета Set-AsmRecoveryAgent

Параметр	Требуется	Тип	Описание
Login	Да	string	Логин пользователя агента восстановления

Пример использования командлета Set-AsmRecoveryAgent:

```
Set-AsmRecoveryAgent -Login "AsmRecoveryAgent"
```

6. Управление службой

Управление службой производится с помощью MMC оснастки «Службы». Для запуска оснастки выполните следующие шаги: Пуск – Выполнить – mmc. В открывшейся консоли управления выберите: Файл – Добавить или удалить оснастку. В открывшемся окне выберите оснастку «Службы» и нажмите кнопку «Добавить» (см Рисунок 2).

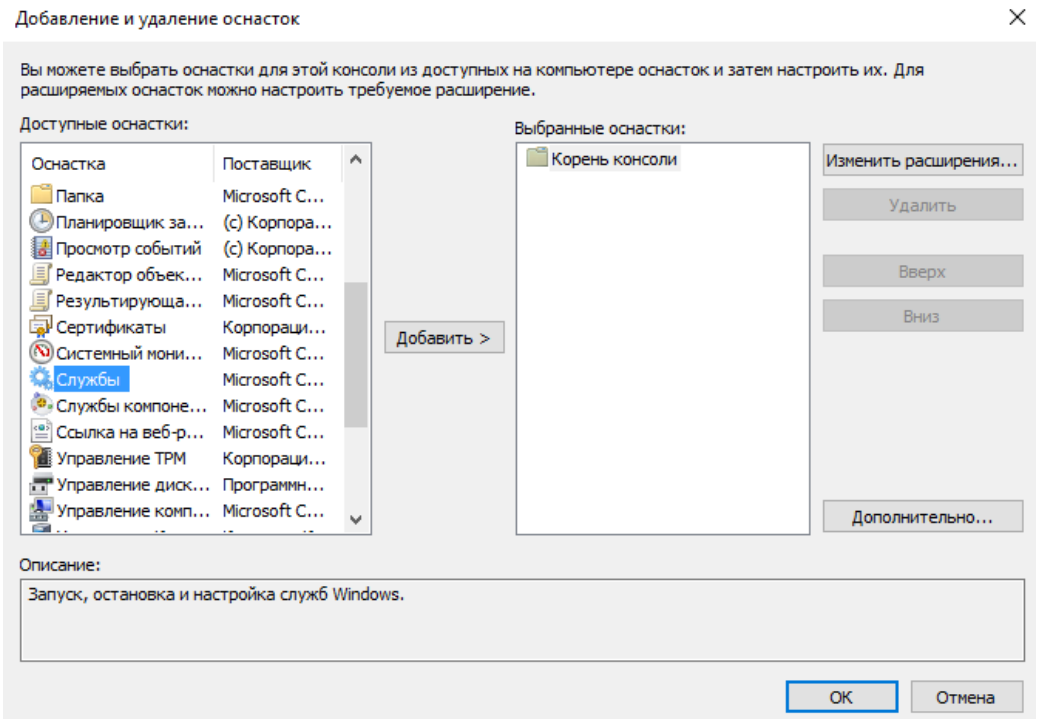

Рисунок 2 – Добавление оснастки «Службы»

По умолчанию тип запуска службы установлен на «Автоматически» (запуск службы при старте Windows). Для успешного запуска службы необходима возможность установления подключения к DSS, на основе параметров подключения к DSS и параметров задач. При возникновении ошибок при старте службы – службы будет остановлена с записью соответствующих сообщений в журнал.

7. Тестовая версия

Для использования тестовой версии необходимо совершить дополнительные действия.

7.1. WebSso stub

Для использования тестовой версии необходимо создать тестовую службу webSso. Для этого необходимо создать папку C:\inetpub\wwwroot\webSso и скопировать содержимое одноименной папки из пакета поставки. Далее необходимо открыть диспетчер служб IIS-> Default Web Site -> (правая кнопка) -> добавить приложение: псевдоним - webSso, физический путь - C:\inetpub\wwwroot\webSso.

7.2. dWeb stub

Для использования тестового модуля dweb необходимо раскомментировать следующие строки в файле C:\Program Files\Crypto Pro\DSS\Asm\WebConfig.xml

```
        <modules>
```

```
            <add name="dweb"
type="DSS.AutoSigner.Web.DWebStub.DWebHttpModule" />
        </modules>
```

При использовании тестовой аутентификации права и группы пользователей выдаются на основе префиксов в имени. Допустимые префиксы: «u_» - пользователь, «o_» - администратор, «a_» - аудитор. Разрешается использование нескольких префиксов. Так, например, пользователь u_a_user@mail.com будет состоять в группах пользователя и аудитора.