**Отдел за безопасност на движението**

3M, сграда 235-3A-09

Ст. Пол, Минесота 55133-3225 [www.3M.oom/mvss](http://www.3M.oom/mvss)

3M™ СИСТЕМА ЗА УПРАВЛЕНИЕ НА КЛЮЧОВЕ НА КАМЕРА СЪС СРЕДНА СКОРОСТ

РЪКОВОДСТВО НА ПОТРЕБИТЕЛЯ

ИЗДАНИЕ 2.0

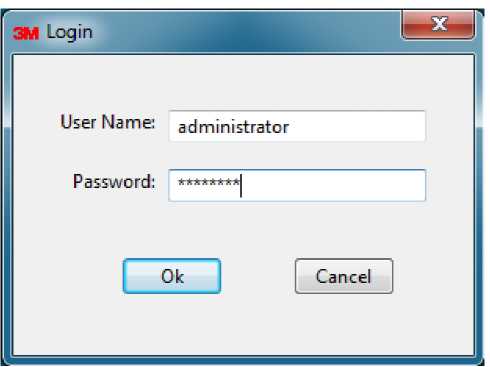
СПИСЪК С ИЗВЪРШЕНИТЕ ПОПРАВКИ

|  |  |  |
| --- | --- | --- |
| ИЗДАНИЕ | ДАТА | КРАТКИ ДАННИ ЗА ИЗВЪРШЕНАТА ПРОМЯНА |
| 1.0 | 17/07/2009 | Първоначална версия |
| 2.0 | 09/07/2013 | Актуализиране на 3М номенклатурата за продукти |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

Настоящият документ представлява последното издание, показано в таблицата по-горе. Автори: Куифенг Хуанг

**1. Потребителски акаунт**

При стартиране на системата за управление на ключове на 3M™ камерата със средна скорост (КМ, позната преди като SpeedSpike система за управление на ключовете) потребителят трябва да се регистрира с потребителско име и парола, както е показано на фиг. 1.

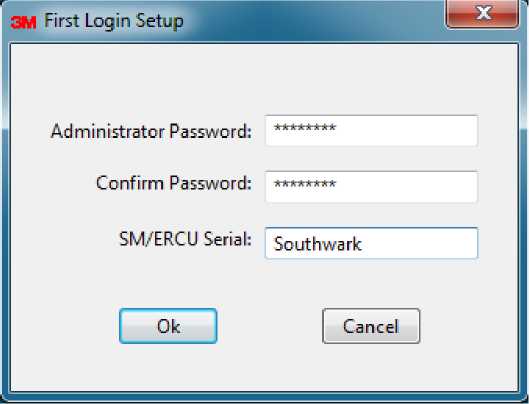


**Фиг. 1 Регистриране в КМ**

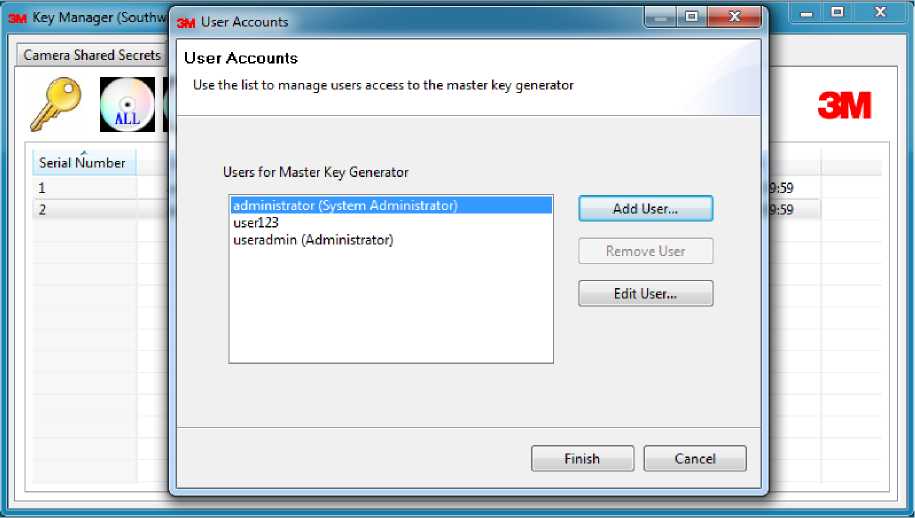
В КМ могат да бъдат зададени три нива на потребителски акаунти, като се следва парадигмата на Windows.

* Потребител
* Разглеждане, подаване на заявки и генериране на камери и споделени тайни
* Разглеждане и генериране на бази с ключове
* Издаване/повторно издаване на споделени тайни и бази с ключове, както и проследяване на историята на изданията
* Редактиране на собствения си акаунт
* Администратор
* Добавя/Премахва/Редактира потребители
* Импортира данни за камери от системата за управление на изпълнението
* Архивира системни данни
* Системен администратор
* Добавя/Премахва/Редактира администратори и потребители
* Вижда исторически паролите на всички издадени CD
* Генерира „възстановен CD“ за системата за управление на сесии (SM)
* Recover system from a backup CD Възстановява системата от архивирания CD

Паролата на системния администратор и серийния номер на SM/ERCU трябва да бъдат зададени при първоначално стартиране на КМ, както е показано на фиг. 2. При натискане на бутона “User Account” на страницата "System Key Store” се отваря потребителският интерфейс за управление на потребителските акаунти, както е показано на фиг. 3.

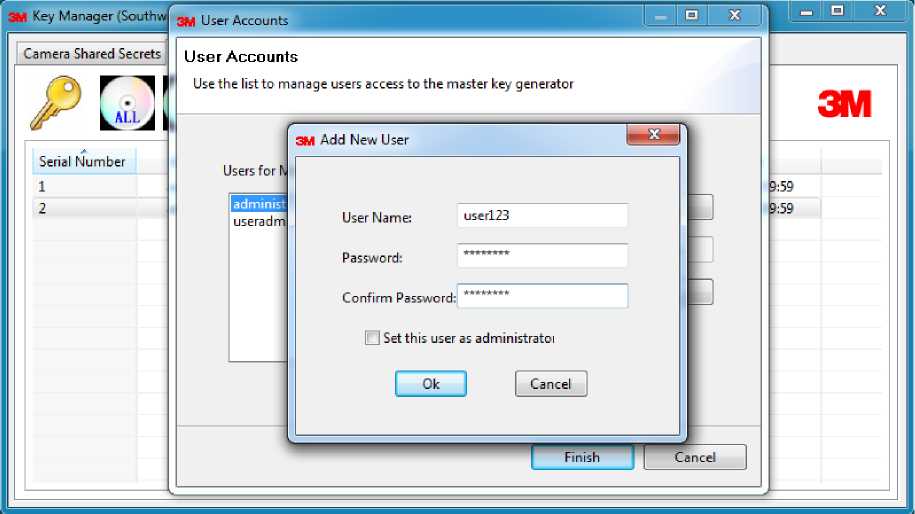


Фиг. 2 Настройване на първо пускане на КМ



Фиг. 3: Управление на потребителските акаунти

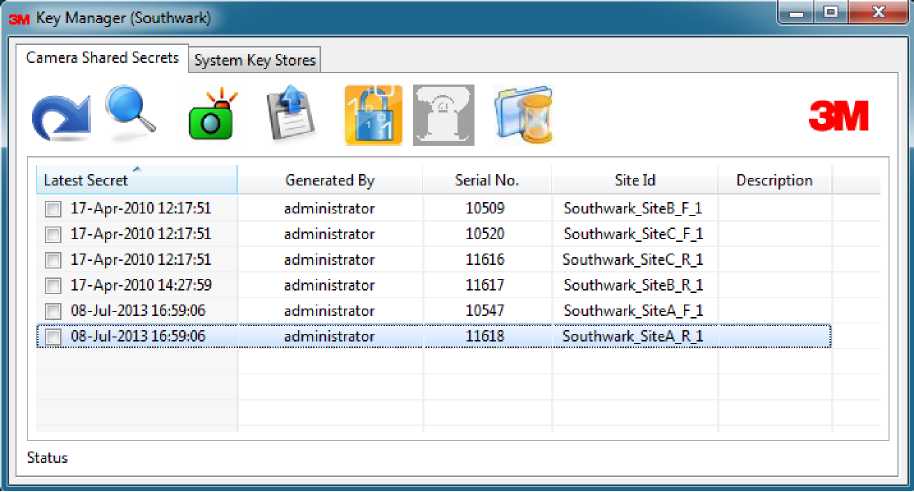
Операциите по добавяне/премахване/редактиране са достъпни са потребител със съответните привилегии. За пример е представена операцията за добавяне на потребител, показана на фиг. 4. За добавянето на нов потребителски акаунт е необходимо предоставянето на уникално потребителско име и парола, както и възможност за добавяне на този потребител като администратор, ако операторът се е регистрирал като системен администратор.



Фиг. 4 Добавяне на нов потребителски акаунт

Заб.: за да приложи извършените промени в потребителския акаунт, операторът трябва първо да натисне бутона "Finish” в страницата за управление на потребителски акаунти, за да излезе от нея.

2. Споделена тайна на камерата

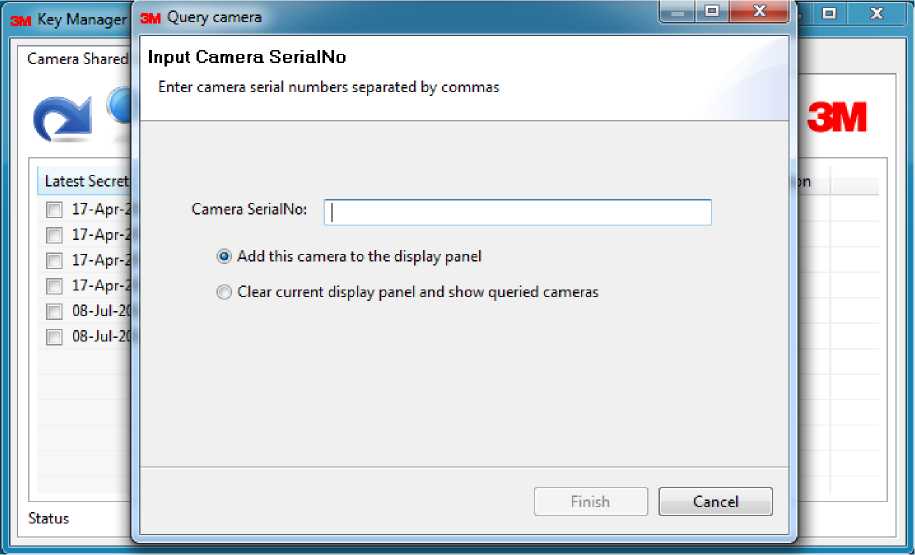


Фиг. 5 Основен прозорец на споделена тайна на камерата

Споделените тайни на камерата представляват част от фундаменталната вътрешно-външна сигурност. Съвместимата споделена тайна трябва да бъде криптирана и запазена, както на камерата, така и в SM.

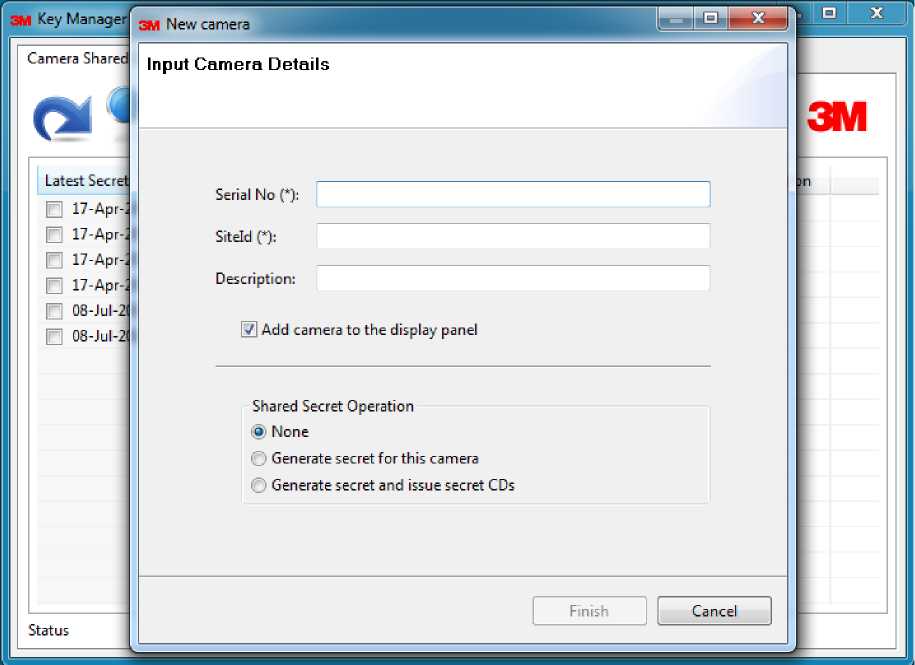
Обобщеното състояние на споделената тайна на камерата е показано на фиг. 5 с бързи бутони за обичайни потребителски операции, които включват:

* "Заеми всички камери”: заема всички камери, въведени в система, и показва техните данни в панел.
* "Заявка за камери”: Както е показано на фиг. 6, изпращане на заявка за данните на въведените камери на базата на серийните номер или серията от серийни номер, разделени с разстояние или запетая. Резултатите могат да бъдат показани в нов панел или с нови камери, добавени към настоящия списък.



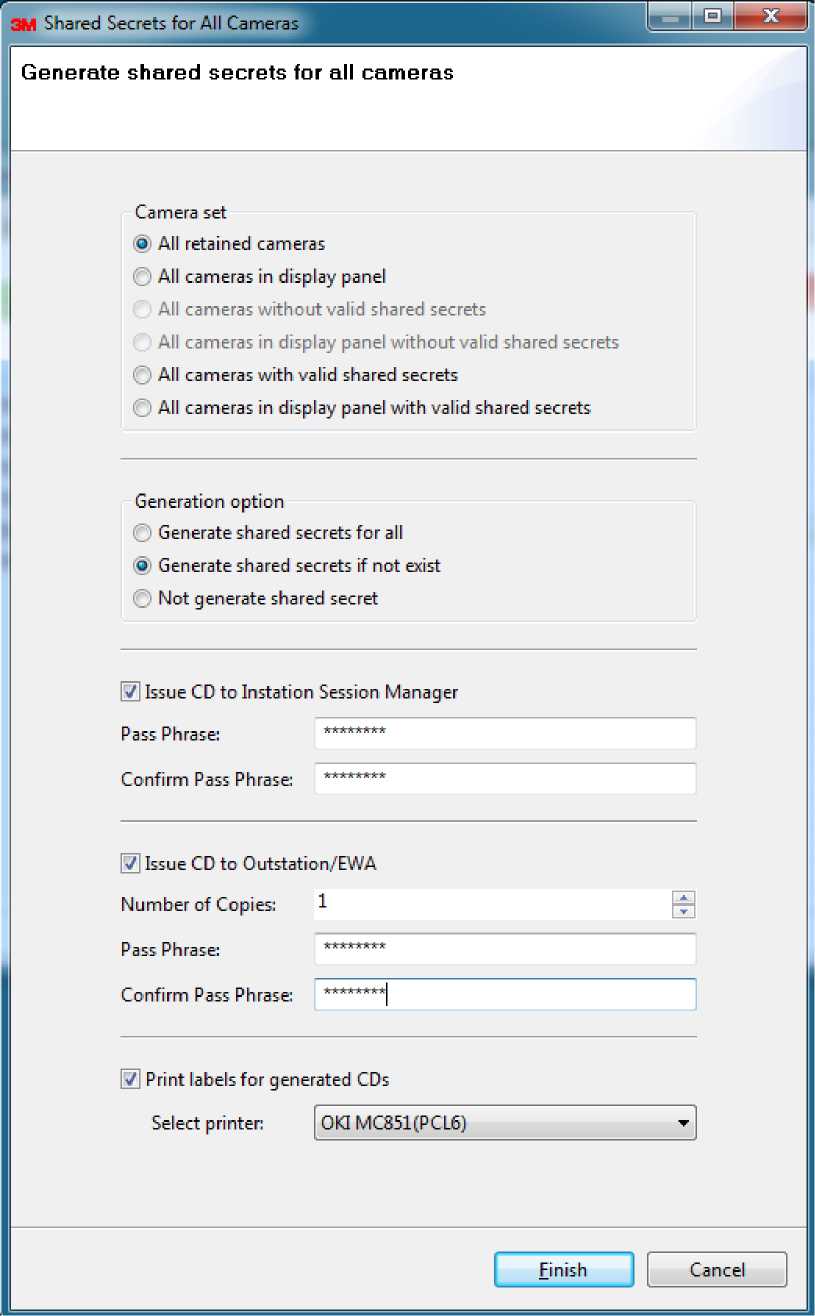
Фиг. 6 Заявка за данни на камера

> "Нова камера”: Както е показано на фиг. 7, КМ разрешава на потребителите ръчно да добавят камери в системата, както им дава и възможност да генерират и/или издават споделена тайна, ако желаят. Ако е зададената опцията "issue secret CDs” (издаване на CD с тайни), на екрана ще се появи допълнителна страница, на която да зададете паролата за защита на издадения CD. За да завършите процеса, просто трябва да следвате указанията на екрана.



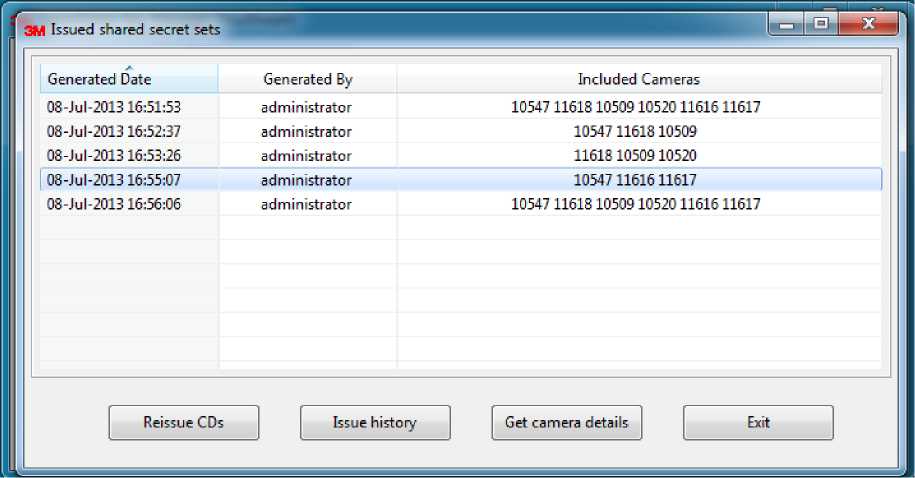
Фиг. 7 Добавяне на нова камера

* "Импортиране на камери”: тази операция е разрешена само за администратори или системни администратори, които импортират данни на камери, идващи от системата за управление на изпълнението (ЕМ) в системата.
* "Тайни за всички”: Цялостна операция за всички записани камери или всички камери, показани в основния панел. Както е показано на фиг. 8, групата камери, включени в операцията, е зададена в първата група с радио бутони, а във втората група радио бутони е включено при какви условия ще се генерира нова споделена тайна за конкретната камера. Операторът може да избере също дали последната споделена тайна за всяка камера в избраната група от камери трябва да бъде издаденa на SM и/или на външна станция, паролите за защита, CD копията, както и дали да бъдат отпечатани етикети за CD на избран принтер.

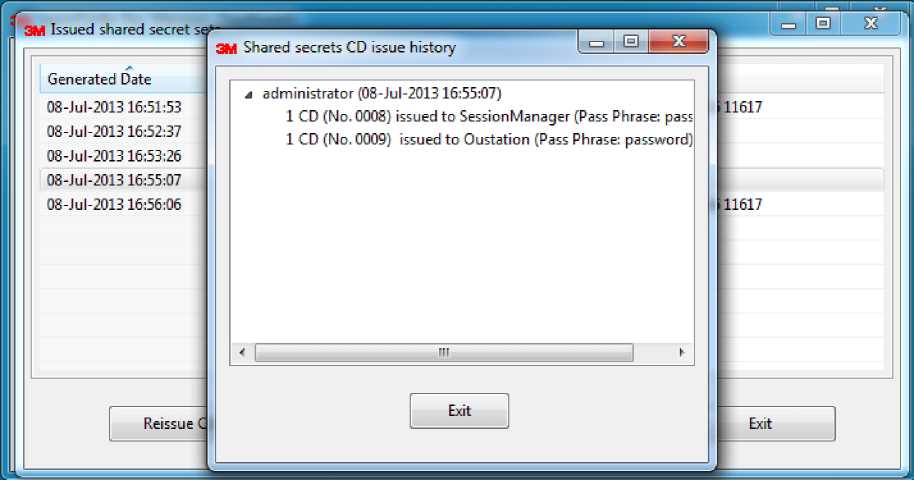


Фиг. 8 Генериране/издаване на споделени тайни за всички

* "Тайни за избрани”: подобно на предходната операция „тайни за всички“, но се отнася само за избраните в основния панел камери.
* "Издадени групи тайни”: При натискане на този бутон, влизате в страницата за управление на всички групи исторически генерирани/издадени споделени тайни, както е показано на фиг. 9. За всяка група може отново да бъде издаден нов CD, включващ точно същата група споделени тайни към SM/външна станция. На екрана се появява предупреждение, ако някоя от включените камери има нова генерирана споделена тайна спрямо момента на генериране на групата от тайни. Операторът може също да направи пълна проверка на историческата информация от издаването на CD, а системният администратор има възможност да провери паролата за всеки CD, ако паролата при регистрация е потвърдена, както е показано на фиг. 10. Операцията, която се стартира с бутона "Get camera details” (Получи данни за камерата) поставя всички данни на камерите в основния панел, като подчертава камерите с актуализирани споделени тайни.

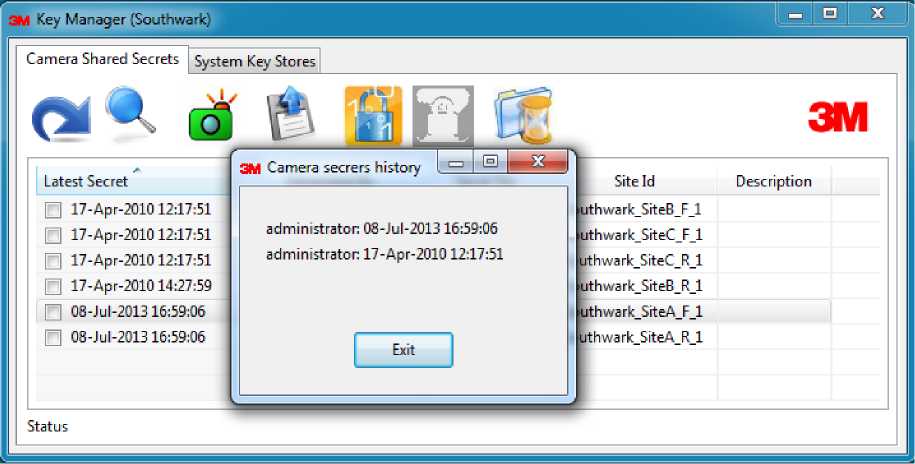


Фиг. 9 Управление на издадените групи споделени тайни



Фиг. 10 Проследяване на историята на издаване на споделени тайни

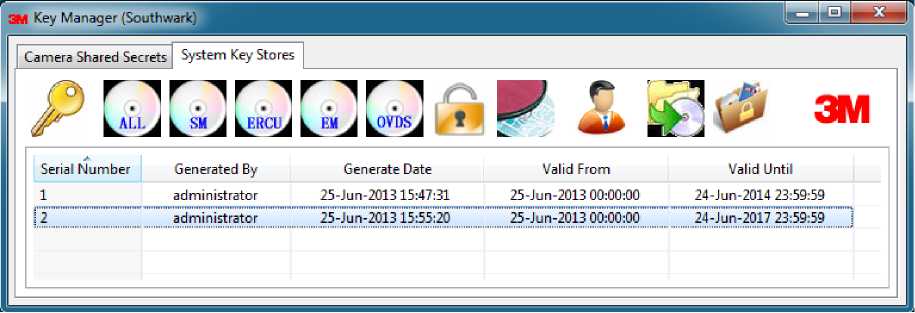
При натискане на десен бутон на мишката на екрана се появява меню, с помощта на което можете да извадите цялата история на генериране на тайни за конкретна камера, както е показано на фиг. 11, или дори да изтриете камера, ако от тази камера до момента не е генерирана споделена тайна.



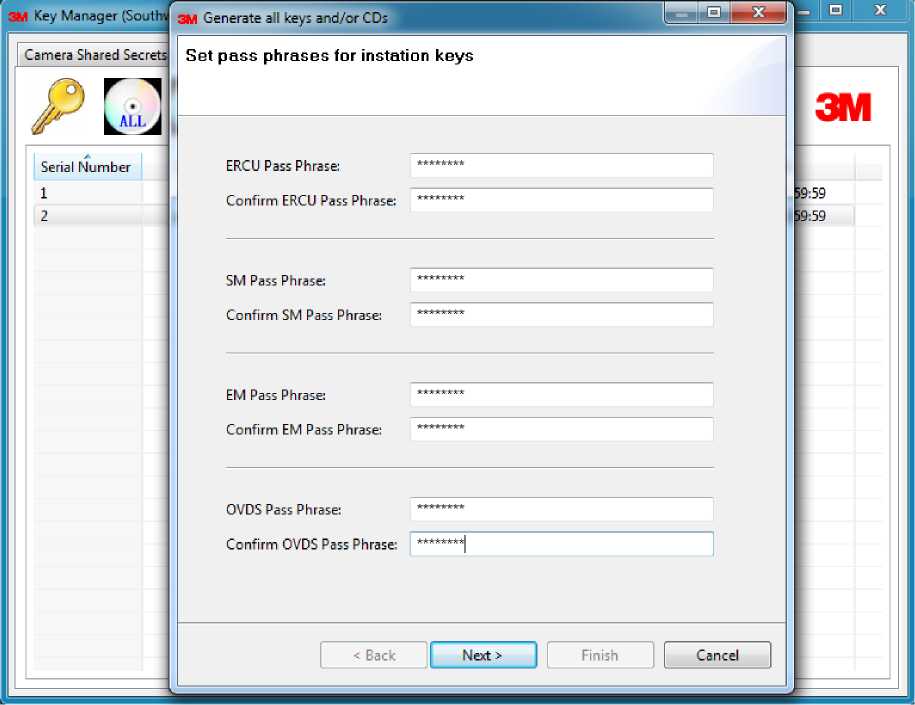
Фиг. 11 История на генериране на споделените тайни на камера

3. Управление на базите с ключове

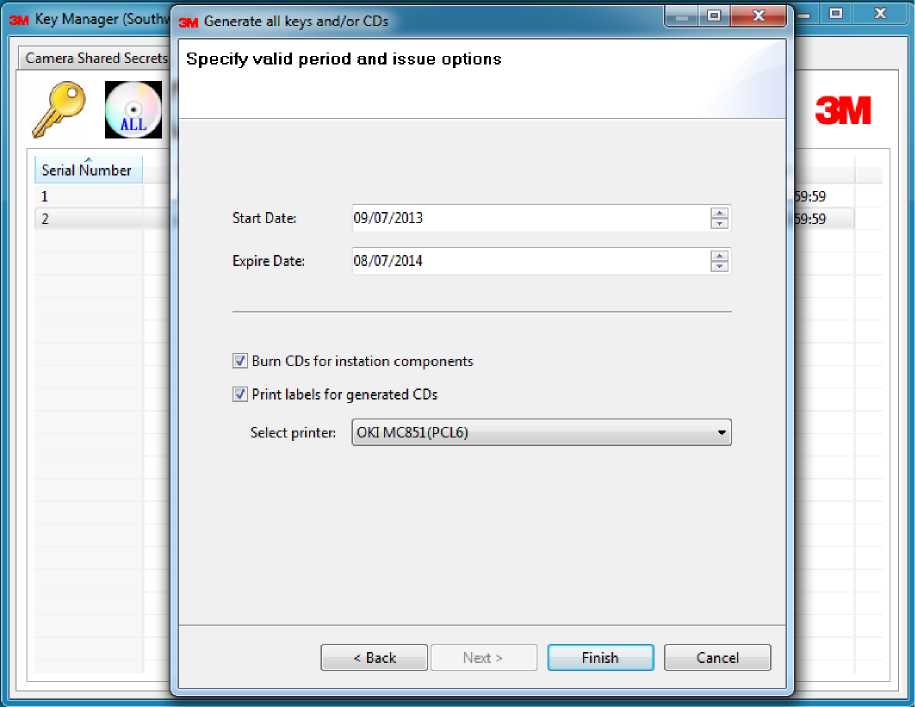
3M™ камерата със средна скорост използва RSA-2048 базирана публично-частна двойка ключове като основа на машина-машина сигурността, както и AES-256 базирани симетрични ключове, като основен механизъм за защита на много критична информация, като споделени тайни на камера и ключове за сесии. Основните функции на системата за управление на базите с ключове включват: генериране на всички двойки ключове и симетрични ключове; поставяне на ключовете в двойки и доставяне до SM, ERCU, OVDS и EM, всяка една разположена в отделна база с ключове и защитена с парола. Обобщаващият екран на системата за управление на базите с ключове е показан на фиг. 12.



Фиг. 12 Обобщаващ екран на системата за управление на базите с ключове



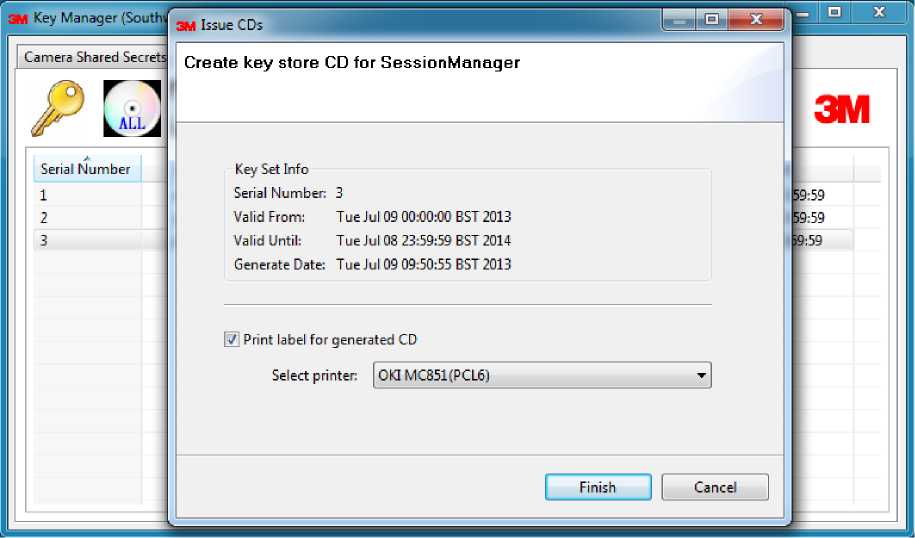
Фиг. 13 Задаване на пароли за всички бази с ключове



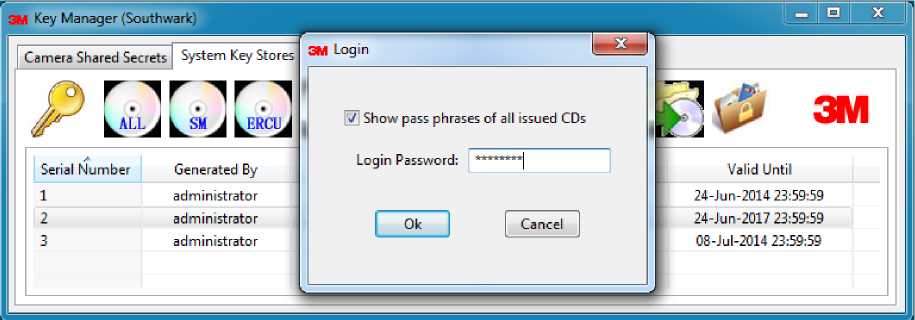
Фиг. 14 Задаване на валидност на базата с ключове и опция за издаване

На фиг. 13 и фиг. 14 е показан процесът за генериране на група ключове. За всяка отделна база с ключове трябва да зададете индивидуална парола. При всяко стартиране на компонент от страна на сървъра/PC (SМ, ERCU, OVDS и EM) се изисква въвеждането на съответстващата парола. Както е показано на фиг. 14, за всички генерирани бази с ключове трябва да се зададе и период на валидност. Вътрешната станция не може да започне изпълнение преди този период на валидност, а след изтичането му трябва да бъде опреснена, за да продължи работа. Съществува възможност да запишете тези бази с ключове на CD и да отпечатате етикети за CD, като следвате инструкциите от изскачащите диалогови прозорци. Впоследствие, ключовете преминават през защитата на мрежата и биват доставяни до машината на вътрешната станция, за да бъдат заредени или актуализирани.

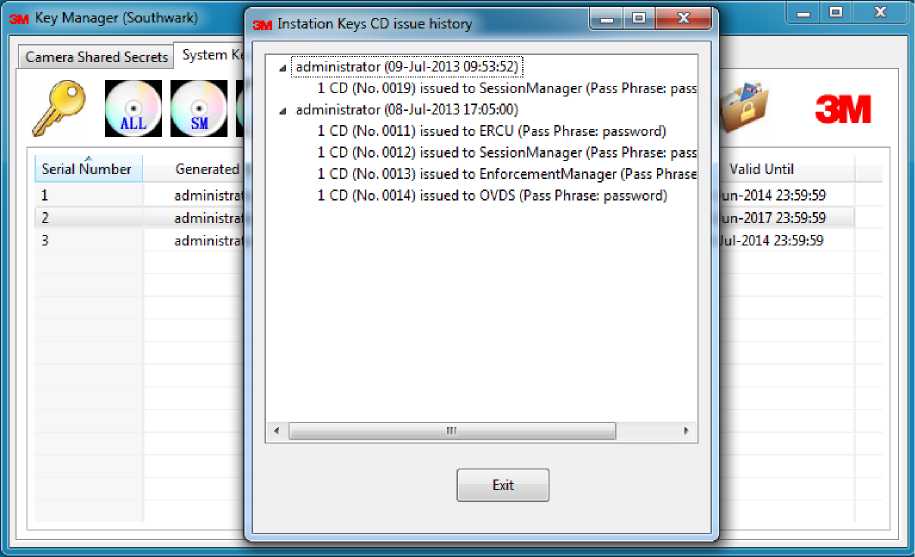
Можете и по-късно да запишете всичките четири или само един CD за дадена генерирана група с ключове. Този процес е показан на фиг. 15, при който базата с ключове се издава със сериен номер 3 към SM. По подобен начин можете да проверите и пълната история на издаване на даден CD за всяка група ключове, а системният администратор има възможност да провери паролата за всеки CD, ако паролата на регистриране е потвърдена, както е показано на фигури 16 и 17.



Фиг. 15 Издаване на CD с база с ключове към SM



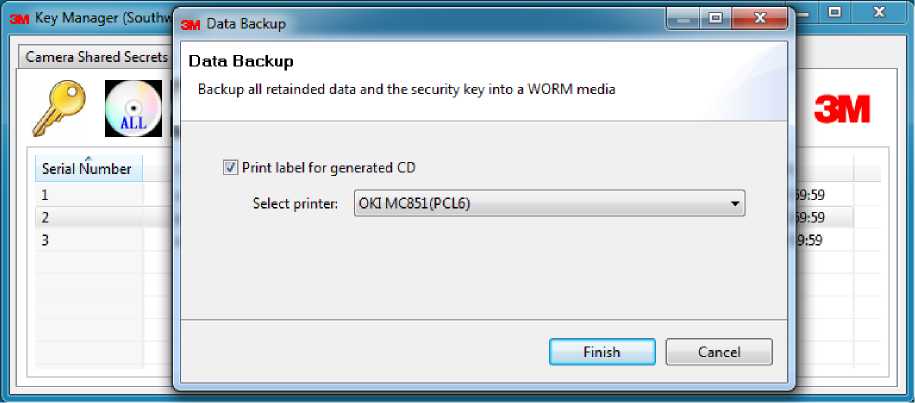
**Фиг. 16 Потвърждаване на администраторската парола**



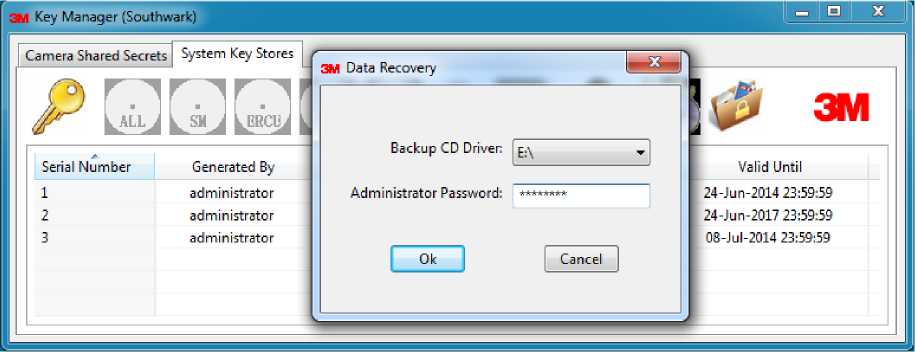
Фиг. 17 История на издаване на базата с групи ключове

Препоръчително е базите с ключове на вътрешната станция да бъдат променяни поне веднъж годишно и да се използват в историческата си последователност. Промяната на база с ключове в SM включва няколко критични операции по актуализиране на записаните споделени тайни и ключове за сесии, които трябва да използват ключове за достъп до старата база с ключове за разшифроване на данни и ключовете за достъп до новата база с ключове за повторното им криптиране. КМ предоставя функция за издаване на специален „възстановителен CD“ за SM. Този CD съдържа всички необходими исторически ключове за достъп и SMDL автоматично обновява системата до настоящата база с ключове, като използва този CD, независимо от това коя база с ключове е заредена в момента или е възникнала грешка с текущата използвана база с ключове за SM.

Дадени бази с ключове и споделени тайни, управлявани от КМ, играят важна роля в системата на 3M™ камерата със средна скорост. КМ предоставя допълнителни функции за извършване на архивиране и възстановяване, които могат да бъдат упражнявани от администратор или дори системен администратор (за възстановяване на данни), както е показано, съответно, на фиг. 18 и фиг. 19. Препоръчително е да извършвате операцията архивиране веднага след генерирането на нова група ключове, както и редовно след това. Възстановяването на данни, обаче, трябва да бъде извършвано само при съществуването на добра причина, както и с професионалната подкрепа на 3М, тъй като съществува вероятност да изгубите част или дори всички промени, направени в системата от изготвянето на архива.



Фиг. 18 Архивиране на данни



Фиг. 19 Възстановяване на данни

Приложение: Конфигурации в KM

Някои конфигурации могат да бъдат зададени във файла $KeyManager/conf/ key-manager.properties, които са показани както следва (можете да игнорирате първата част, ако използвате посочените настройки по подразбиране):

#Конфигурациите трябва да са същите като тези в EWA (във файла ewa.ini):

ewa.secret.file = site\_100.enc

ewa.camera.serialNo.column = 1

ewa.primary.secret.column = 2

ewa.trial.secret.column = 3

#Посочване името на CD-записвачка cd.writer.device = d: