

## **PrivateServer FAQ**

***Q: How can I recover from a scenario where I have only a backup file and there are no init or startup cards and the appliance is not working – but I do have an alternate appliance?***

**A: When creating the Startup and Init cards using the PSVGenCards.exe utility you should write down on paper (and secure it in a safe!) the two components of the SVMK (one is requested when creating the Init card and the other when creating the Startup card). This will create a new set of Startup and Init cards that will be used for Initializing and restoring a backup to a different PrivateServer in case of a damaged server or/and loss of the original cards.**

**Note: when generating the startup card you can make a backup.**

**Please note the SVMK of the server that created the backup file must be identical to the SVMK of the target PrivateServer or the restoration process will fail.**

**In order to create the cards you need to run the utility PSVGenCards and do the following:**

- **You can skip the Root card creation.**
- **In the Init prompt it is important to enter the exact SVMK part that was entered when creating the original Init card.**
- **In the Startup part it is important to enter the exact SVMK part that was entered when creating the original cards.**
- **Enter the details of a user who will be permitted to connect to the server without a card following the initialization process.**

**The rest of the information is irrelevant since the only case we are concerned with here is the creation of a card to restore backed up data. For example, if required, you may enforce authentication for this user, but keep in mind that you will have to create a media for him before he can connect, and since you are about to restore the database from the backup file, it is not really necessary, (this user may not even exist in the restored database, and his access level will anyway be determined by the backup file, after it is restored).**

***Q: In the Synchronization utility, what is the difference between synchronizing keys with the SVMK to synchronizing keys with KEK?***

**A: KEK (Key Encryption Key ) is a key that is used to encrypt other keys in order to transfer them to a different location .**

**SVMK is the key that is used to encrypt the database in the PrivateServer.**

**Every PrivateServer contains a certain SVMK.**

**PrivateServers that were initialized with the same Init and Startup cards are using the same SVMK.**

**When exporting keys that were encrypted with SVMK, these keys can only be transferred to a server that had been initialized with the same Init and Startup cards.**

**When exporting keys that are encrypted with KEK it is possible to transfer them to servers that do not contain the same SVMK.**

**This means that you can transfer keys to a different environment, but the server must include the same KEK for decrypting the key.**

**In order to do that you can load the KEK to all your servers or you can generate it on a certain server and then transfer it to another.**

**Please note that if the key is marked as READ\_KEK you can also get its value by SVMK but if the key is marked as READ\_SVMK you can't get it by using any of the KEK keys.**

***Q: What card types can be used as Init and Startup cards?***

**A: Basically AR provides 2 types of smartcards:**

- 1. MCOS cards- there is an indication named "Gemplus" on the smartcard chip.**
- 2. PrivateCards - a high security PKI based smartcard with a 32/64 KB memory capacity. The card performs all the sensitive functions on the chip itself, providing users with a significantly stronger authentication mechanism.**

**The MCOS smartcard chip is rounder in shape, unlike the PrivateCard that is square-shaped but has round edges.**

**When creating cards to be used as INIT or STARTUP, MCOS cards MUST be used.**

**When generating cards for users that will connect from the PrivateServer client machine, you may use both types of the cards providing the client machine is using CryptoSafe for the smartcard reader. If the client machine has PrivateSafe, you can only use PrivateCards.**

***Q: What is the difference between a secure network and NON-secure network?***

**A: Secure networks and non-secure networks are definitions that should be determined by the PrivateServer operator.**

**A "secure network" means that the organization has taken measures to limit access to this network. For example, to be able to get a certain IP address you need to access a certain building. Another example for a secure network is a cross cable between a client machine and the PrivateServer.**

**A "non-secure" network means that the organization has no control over the network and it can't limit access from this network. For example, a PrivateServer that is connected to the internet.**

**Another example, a PrivateServer that is located in a bank. If only a single computer connects to the PrivateServer you can define the network as "secure" since no other computer can access the PrivateServer, but if all the bank's employees are able to connect to the PrivateServer you should define it as "non-secure" since you want the user authenticated when connecting to the PrivateServer.**

**Each user in the PrivateServer database has an access level that determines whether the user must arrive from a secured network, (or not).**

**If it is defined for a certain user that he must connect from a secured network, you need to add/define in PrivateServer's console, in the "secured networks", the network he is connecting from.**

**PrivateServer has 2 NICs, one is defined as secured and one as non-secured by default. You can define both of them as secure/non-secure.**

***Q: What types of access are available?***

**A: There are 5 access types:**

- 1. Users may connect from a non-secure network without the need for authentication (authentication is enabled by a key that is password protected).**
- 2. Users must connect from a secure network but without the need for authentication.**
- 3. Users must connect with authentication from a non-secure network.**
- 4. Users must connect with authentication but only from a secure network.**
- 5. Users can't connect to the PrivateServer.**

**An authenticated session means that the user uses a certain media to connect to the PrivateServer.**

**The media stores the user's authentication private key.**

**The media can be a smartcard, a Minikey or a key file.**

**In a production environment, AR recommends not to delete users but to change the user's access level to 5. This will prevent the user from connecting.**

***Q: What do I have to do in order to backup a user?***

**A: Create a backup user with the same authorization mask, same access level, same certifier, etc. The certificate's lifespan of the backup user should be longer than the certificate's lifespan of the original user. This backup user must have the same access rights to keys (owner/user) as does the original user**

**This backup card will help the customer to handle a case where initial cards are lost or damaged, or if the original user can no longer connect since his certificate has expired.**

**If the certificate's lifespan of the original user expires, the backup user can connect and renew the certificate, so that the original user is able to connect.**

**In this case the backup user will be able to connect to the server and perform all operations that the original user was allowed to do.**

**It is highly recommended to backup your important users. If you don't, and the user's media is lost or damaged, you might not be able to connect to the server or use your keys.**

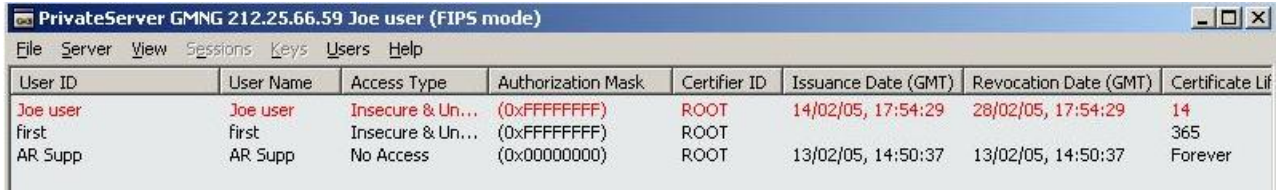
***Q: What must I do in order to maintain this backup user?***

**A: If you add keys /grant rights to keys to original users or generate keys with the original user, you will have to do the same with the backup user, so that he has the same rights to the same keys.**

**Keep in mind that you will need to renew his certificate before it expires , so its access to PrivateServer will not be denied.**

**Q: In PrivateServer Admin (Gmng.exe) I see users with red characters – what does it mean/ what should I do?**

**A: If the user's certificate has expired, OR there are 14 or less days until the certificate WILL expire, you will see the user's details in red characters:**



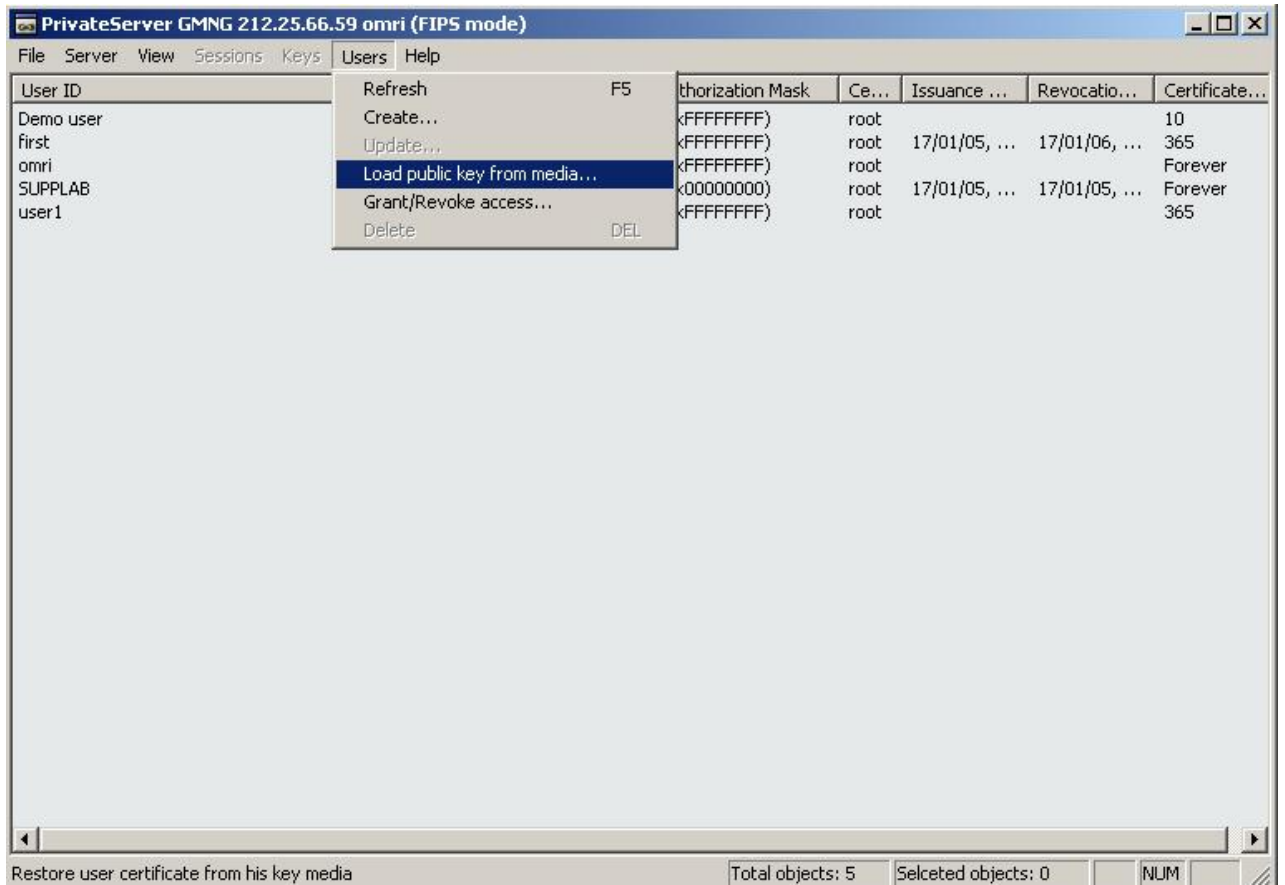
User ID	User Name	Access Type	Authorization Mask	Certifier ID	Issuance Date (GMT)	Revocation Date (GMT)	Certificate Lif
Joe user	Joe user	Insecure & Un...	(0xFFFFFFFF)	ROOT	14/02/05, 17:54:29	28/02/05, 17:54:29	14
first	first	Insecure & Un...	(0xFFFFFFFF)	ROOT			365
AR_Supp	AR_Supp	No Access	(0x00000000)	ROOT	13/02/05, 14:50:37	13/02/05, 14:50:37	Forever

In this case you should recertify the user.

In The MNG (a command line tool) menu – select option 4:

```
Enter choice:
1 - create user
2 - list users
3 - list keys with key access
4 - load certified public key from media
5 - get user certified public key
6 - get csv's certified public key
7 - list sessions
8 - revoke user
9 - shutdown
10 - backup
11 - restore
12 - load file
13 - create/delete dir/file
14 - download logfile
15 - reset logfile
16 - update user record
17 - kill session
18 - grant/revoke key access
19 - delete key
20 - get server info
21 - msgctl
22 - func msgctl
23 - List_Functions
24 - List Modules
25 - Key Suspension
0 - exit
```

In GMNG you need to select "Load public key from media" in the Users menu.



**NOTE: AR does not recommend deleting and recreating users, mainly because if a key is linked to just one user, when deleting the user all his keys become unusable – it's preferable to lock access to a user.**

**Q: Why, when I open the PrivateServer log file via PrivateServer Admin utility (GMNG.exe) (Server ->view log file) I see in notepad that the log appears to be empty?**

**A:**

1. Check from another client station to see if the log file appears.
2. Try to retrieve the log file via MNG and open it with a different viewer (not a notepad).
3. Check that you have enough HD space.
4. Check the PrivateServer's console when trying to retrieve the log . If the counter numbers are increasing, a log file is sent to the client (not necessarily reaching it...). Please note that this requires viewing the PrivateServer console while retrieving the log file.

**Q: What is the PrivateServer's port number?**

**A:** The PrivateServer listens to incoming connections at port 1024.

**Q: How do I reload the DLM's to the Cryptosafe reader?**

Sometimes the CryptoSafe reader doesn't seem to be working. At other times it doesn't work with PrivateCards but just with MCOS smartcards or you may be getting some sort of error or inconsistent behavior from the reader. In most cases these problems are solved by reloading the CryptoSafe's DLMs.

1. Run DL.exe utility to see what DLM's are loaded.  
A correct output should be:

Active RAM program: autoexec (Version 10.1), 3 blocks are loaded.

```
N Ver Id
= == =====
0 10.1 autoexec
9 1.6 RSA10
14 1.1 SCreset-
```

2. Reload the DLM's with the Screset.bat utility.
3. Verify that they are indeed loaded (step 1).
4. If they have not loaded successfully, try replacing the CryptoSafe reader.

***Q: What is the difference between a key owner and a key user?***

**A: The key's user can perform cryptographic operations with the key (i.e., encrypt, decrypt, sign, verify).**

**The key's owner can get the key's value (as long as it's not Read Locked). He can delete the key and modify sensitive attributes of the key.**

***Q: Can the log format be changed?***

**A: No. Since PrivateServer's internal software underwent FIPS 140-1 level 3 certification process, it is not possible to change the log format.**

***Q: Can I change the time of the PrivateServer? Can it get the time from an NTP server?***

**A: No, and there is no need to do it.**

**The internal CryptoSafe on the PrivateServer has an internal clock.**

**Before leaving AR's Manufacturing, this internal clock is synchronized with GPS clocks, which causes the clock's deviation to be one second per year (on the average).**

**Special scenario:**

**You encountered a problem when trying to boot PrivateServer.**

**The scenario is:**

**When the PrivateServer boots it goes thorough all the phases -**

Phase 1

Phase 2

Phase 3

.

.

.

Phase 9

**And it stays stuck on phase 9.**

**Normal boot messages display following phase 9.**

**System starting...please wait...**

**Followed by a PrivateServer menu.**

### **Solution**

**A. If the VGA card is in the AGP slot.**

**Open the box and move the Ethernet card that is defined as LAN-0 to the middle PCI slot (one PCI slot to the left).**

**B. If the VGA card is in a PCI slot.**

**Exchange locations of the PCI slots between the Ethernet card that is LAN-0 and the VGA card, so the LAN 0 is in the middle PCI slot.**

**C: It can happen also if the network card is loose. Contact AR support for more information.**

**Q: There are a lot of messages in the log file, such as:  
" App error user: Anonymous addr: xxx.xxx.xxx.xxx fun: 70 rc:  
168" but users can login to the server. What do these  
messages mean?**

**A: This error is written to the log file any time an authenticated session is established and the PrivateServer is in a FIPS mode.**

**Function 70 is get\_csv\_version.**

**Return code 168 means csv\_anon\_not\_allowed - this function cannot be executed as anonymous.**

**In the past (prior to PrivateServer version 3.0), users were allowed to access the PrivateServer for specific functions without specifying their user ID. The functions that allowed such access were called "anonymous functions".**

**In v3.0 and later releases such access is not allowed if the PrivateServer is set to work in a FIPS mode.**

**We used an API call from the client side during any "open session" operation in order to make a distinction between working with the old client procedure or with the new FIPS client procedures. This is the reason you are getting this message written to your log. This indicates you are working in a FIPS mode.**

**We will change the mechanism in the next version (4.0) of PrivateServer to print a more accurate message and not an "error" message.**