Process for Initial Keylogger Training Qualification

3/3/2023

Prepared by the Operations Department Training Committee _____

Definitions

- **Keylogger Training (Training)** – Applied training of the "Issuing Keys in the Main Control Room" section from *The Keylogger & You* reference manual.
- **Keylogger Trainee (Trainee)** – A member of the Operations Department who will be receiving Keylogger Training.
- **Keylogger Trainer (Trainer)** – A member of the Operations Department who is Keylogger Qualified and will be instructing the Trainee.
- **Keylogger Qualified (Qualified)** – A member of the Operations Department that has completed Keylogger Training and received Department Head Signoff. Those who are Keylogger Qualified are authorized to issue keys in the Main Control Room and act as a Trainer.
- ***The Keylogger & You* Signature** – The Trainee signs that they have read *The Keylogger & You* reference guide.
- **Enclosure Key Transaction** – The act of entering an enclosure key barcode number and Fermilab ID number into the Keylogger program, and either issuing the key to the person requesting the key, or not issuing the key due incomplete training requirements.
- **Transaction Signoff** – The Trainee participates in fifteen (15) enclosure key transactions with the Keylogger under supervision of personnel who are **Keylogger Trainers**.
- **Department Head Signoff** – The Operations Department Head, Deputy Head, or designee may sign off a Trainee as Keylogger Qualified upon completion of this Training.

Purpose

The purpose of this process is to outline the steps required for a Trainee to become Keylogger Qualified to issue keys to personnel in the Main Control Room (MCR) using the Keylogger program.

Prerequisites

A Trainee must have accrued three (3) months of service time prior to beginning the Qualification process. During that three-month period, the Trainee can use the Keylogger under supervision of a Qualified Trainer to begin becoming acquainted with the system. No Transaction Signoffs may be obtained by the Trainee during this time.

A Trainee must read *The Keylogger & You* reference guide to become familiar with the Keylogger program, and sign *The Keylogger & You* signature box, located in the Keylogger binder, confirming the Trainee has read the material. The Trainee must be aware of the current status of enclosures at the time of the enclosure key transaction. Ideally, the Trainee also has familiarity with basic computer troubleshooting.

Training Process

In order to become Keylogger Qualified, a Trainee must successfully perform fifteen (15) enclosure key transactions under supervision of a Keylogger Qualified Trainer. For each successful transaction, the Trainer will give the Trainee a Transaction Signoff. Once the Trainee has completed the required fifteen (15) signoffs, the Trainee will receive the Department Head Signoff, certifying the Trainee as Keylogger Qualified.

Training Conditions

The preferred condition for Keylogger Training is when the Keylogger program and computer are running normally, with the training database recently updated. Preferably, all fifteen (15) enclosure key transactions are not all in close succession. Note: Maximum of five (5) enclosure key transactions may be for the same enclosure. Thus, issuing keys for a minimum of three (3) enclosures is required for Training purposes.

Any deviation from the preferred conditions should be discussed with the Crew Chief and Trainers, prior to Training, to ensure the principles of the Training are not diminished.

Training for Qualification is allowed for enclosure key transactions only. For example, successfully issuing an AC4 key will not be eligible to receive a Transaction Signoff.

Training is not permitted on “Long-term Shutdown” keys, which are available during a period of maintenance activity that spans the course of several months. These keys are handled exclusively by the Operations Duty Assistant.

Training Responsibilities

Keylogger Trainer

- A Keylogger Trainer may sign off a Trainee in the Transaction Signoff box upon the completion of each enclosure key transaction.
    - It is the responsibility of the Trainer to verify the enclosure key transaction has ended in either of the following outcomes:
        - The Keylogger program successfully checks the training of the person requesting the key, finding no problems with the training of the person requesting the key, and logging out the key in the “Keylogger - Outstanding Keys” list.
        - The Keylogger program identifies an out-of-date or missing training requirement, and the enclosure key transaction completes *without* issuing the key to the person requesting the key.
- It is the responsibility of the Trainer to verify the Keylogger program and computer are in working order prior to training.
- It is the responsibility of the Trainer to ensure that the area covered by the requested enclosure key is prepared for access prior to allowing the Trainee to perform an enclosure key transaction.
- It is the responsibility of the Trainer to ensure the Trainee is following all instructions and dialog boxes presented by the Keylogger program.

Keylogger Trainee

- A Keylogger Trainee must sign off that they have read *The Keylogger & You* reference guide.
- It is the responsibility of the Trainee to ask questions to the Trainer when they are unsure of the response required of them from the Keylogger program.
- It is the responsibility of the Trainee to understand and follow all on screen pop-up notifications displayed by the Keylogger program.

3/3/2023 V2.0

The Keylogger & You

A Guide to Using the Keylogger & Issuing Keys

Managed by Fermi Research Alliance, LLC for the
U.S. Department of Energy Office of Science
www.fnal.gov

U.S. DEPARTMENT OF ENERGY | Office of Science

Table of Contents

Introduction

The following document introduces the Keylogger program, which is used by the Operations Department to issue keys to qualified personnel.

Purpose of the Keylogger

The Keylogger is a program that records the transaction of keys issued by the Operations Department to on-site employees, contractors, and visitors for access to areas on the Fermilab campus. It displays a list of keys that are currently issued (*Figure 1*), maintains a transaction history for each key, and cross-checks a copy of the TRAIN Database for an individual's training to ensure it is up to date at the time of the transaction. The Keylogger contains a database of the keys and their assigned Rules, which govern what training is necessary to successfully issue each key.

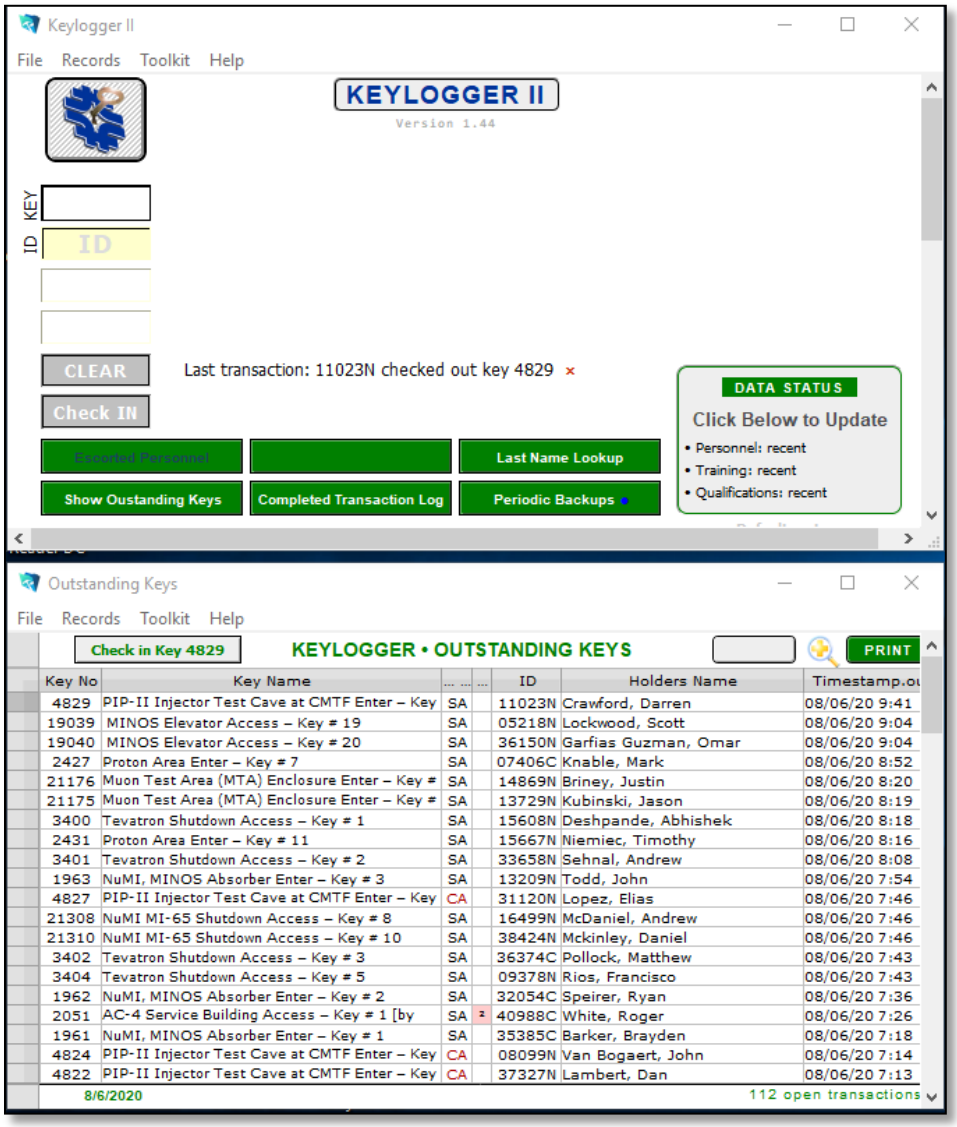

Figure 1

The TRAIN Database

The TRAIN Database contains a list of laboratory-required training courses, which is used along with an individual's Individual Training Needs Assessment (ITNA) to create an Individual Training Plan (ITP). A person's ITP lists the training they are required to complete as determined by their supervisor. The TRAIN database is maintained by ES&H.

When the Keylogger updates its database of training data, it queries the TRAIN Database for all current Fermilab personnel and their training, and saves a copy of it to the Keylogger computer. Since the Keylogger has all of this data onboard, and is connected to backup power, it will still function in the event of power or network outages.

When a key transaction occurs, the issuer (typically an Operator or the Duty Assistant) enters the barcode number of the key and the Fermilab ID number of the person being issued the key. The Keylogger checks its copy of the individual's training against the Rules for the key and reports any discrepancies. If there are no discrepancies, the Keylogger will log the key out, recording the time and to whom the key was issued in the "Outstanding Keys" list.

Updating the Keylogger

To update the Keylogger's data:

1. Click in the grey box marked "DATA STATUS" (*Figure 2*) or click the "Toolkit" menu and select "Update Training Data" (*Figure 3*).
2. The Keylogger will then query the TRAIN Database and completely refresh its local copy of personnel and their training data. This process takes about 45-seconds to complete.
3. A dialog box will pop up once the process is completed stating, "The Training Information is up to date" and the DATA STATUS box will display "recent" as the status for each item. As time goes on, the box will display how old the data is and will be highlighted once it reaches 3 days, reminding personnel to do an update.

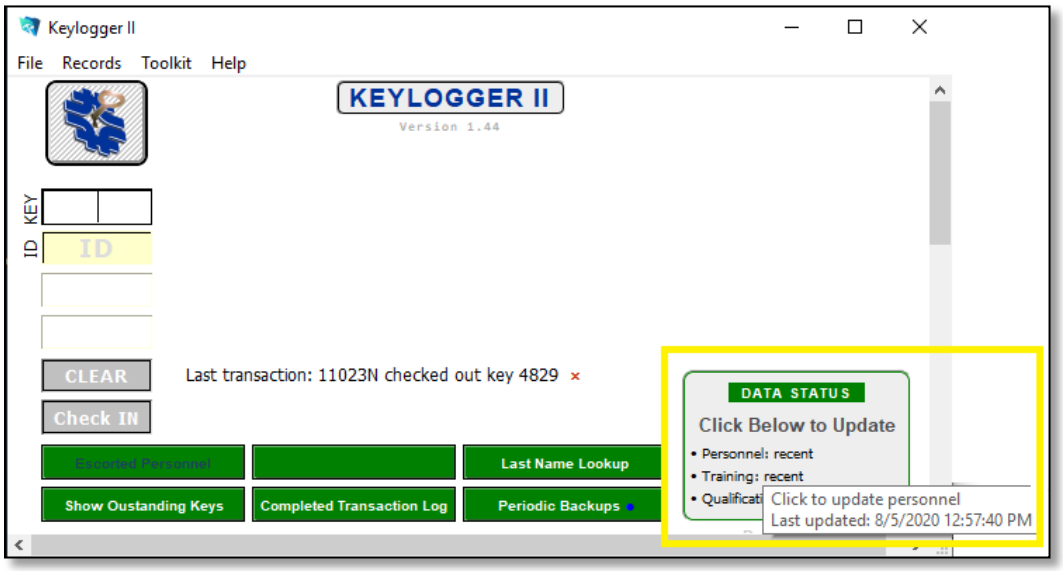

Figure 2

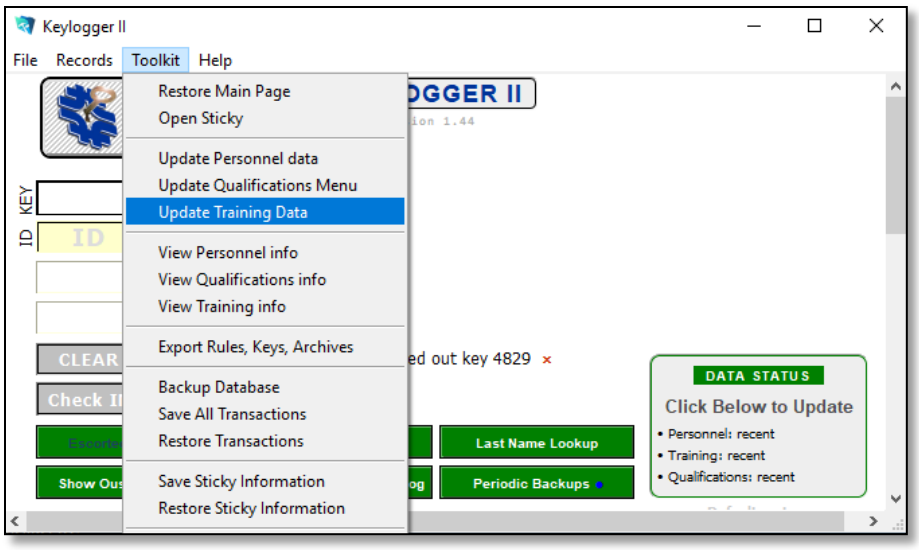

Figure 3

Issuing Keys in the Main Control Room

1. Ask where the person would like to go and determine which key(s) will be necessary.
2. Determine if there are any restrictions and/or approvals that are required before issuing the requested key and follow through with those requirements. See **Area Restrictions and Special Alerts** below for more details.
3. Obtain the key(s) to be checked out. Keys in the MCR are in key trees or hanging on hooks.
4. Input the key barcode number and the requestor's ID number into the Keylogger in the boxes labeled "key" and "ID", then press "Enter" on the keyboard.
    a. If the key is the first to be issued from a set of enclosure keys, the Keylogger will prompt for the type of access being made. Select either *Controlled* or *Supervised*. If you're unsure of the type of access, stop and ask.
    b. If there are special permissions required to obtain the key as determined in step 2 (for example, requiring RSO approval), the Keylogger may show a pop-up prompting confirmation that the permissions were obtained.
5. The Keylogger then checks the Rules for that key against the requestor's training.
    a. If the requestor is flagged on missing or out-of-date training, you will see a large red **NO!** next to the question **ALLOWED?** (*Figure 4*). Pop-up windows will appear, detailing the problematic TRAIN Course IDs. If this happens, **STOP**. Hovering the mouse cursor over the *Training* Key box in the *Not Qualified* Pop-up window will allow you to see all pertinent TRAIN Course IDs and their corresponding names (*Figure 5*).

Figure 4

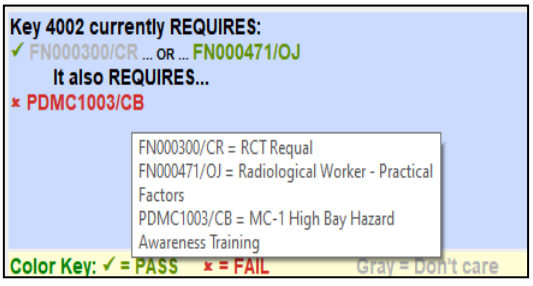

Figure 5

i. Check the requestor's Individual Training Summary (ITS) on the TRAIN database online. You can find the Training ITP link on the Operations Department home page, under Operator Resources.
ii. If the training is missing or out of date on the ITS, inform the requestor that they do not have the proper training for the key. **DO NOT** hand over the key(s). It's possible that the key transaction process might end here, with no key being issued. In that case, click the FAIL! Button to cancel the key transaction and return the key to its key tree or hook.
iii. The Keylogger can Override the training that is being flagged and log out the key to the requestor anyway (pop-ups shown in *Figure 6*). **This is only done on a case-by-case basis with explicit advanced permission from the RSO or DSO**. If advanced permission has been obtained, click *Override* on the NOT QUALIFIED pop-up, and fill out the entire Overriders pop-up with complete information of who authorized the override, the name of someone who double-checked the override, and the full reason for the override. If there has been no explicit permission provided by either the RSO or DSO, you should not Override any training for any reason, and instead click the FAIL! button to cancel the key transaction.

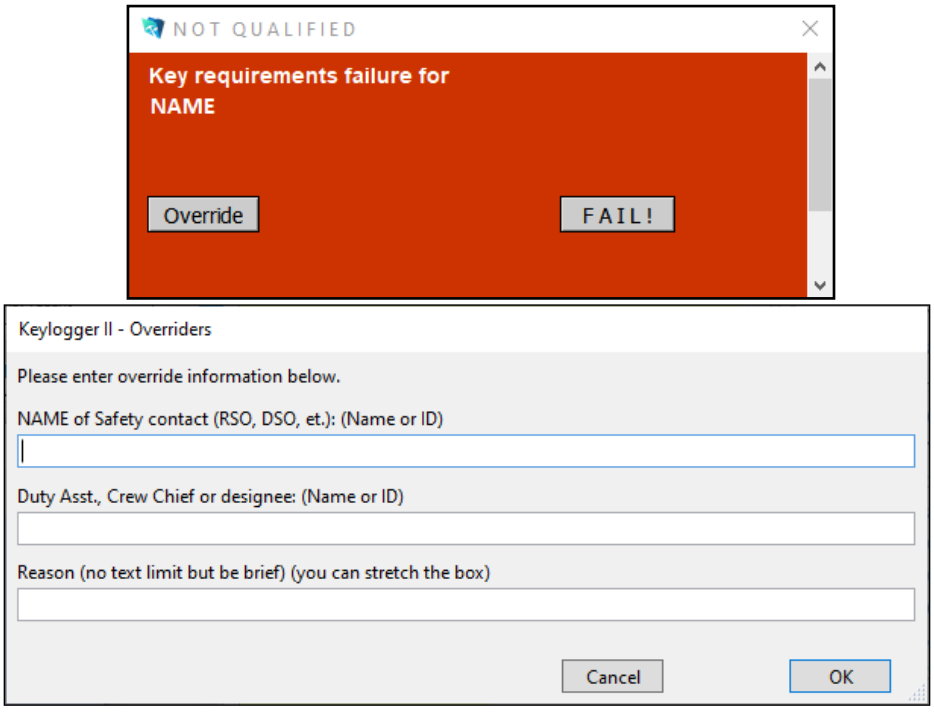

Figure 6

iv. If the training is up to date on the online ITS, update the Keylogger Training Data (as described in Updating the Keylogger) and attempt the transaction again.
    1. If it fails again, consult the Duty Assistant or Crew Chief.
    2. If does not fail, no Keylogger pop-ups will appear. At this point, you can continue with step 6.

6. **Wait** until the Keylogger displays the key in the "Outstanding Keys" section (*Figure 1*). Once the key transaction is recorded there, hand the key to the requestor. Repeat steps 1-6 for each key.

Remember

- At least one enclosure enter key from every set must remain in the key tree to allow access in an emergency.
- **Maintain possession of the key** until the transaction is recorded in the "Outstanding Keys" section of the Keylogger. A key is only considered to be signed out once it appears in the "Outstanding Keys" section.
- If you are ever unsure about what the Keylogger is doing or what the requestor is asking, **STOP** and ask a more senior member of the Operations Department.
- There is always time to ensure the key issuing process is completed properly. If the key requestor has a problem with waiting, inform the Crew Chief.
- Do not feel pressured to check out a key. If you are not comfortable, or do not feel it is safe, inform the Crew Chief.
- Selecting *Controlled* or *Supervised* when issuing the first enclosure key of a set simplifies the training requirements for all subsequent keys issued in that set, since Controlled Access checks are not required when making a Supervised Access.
    - If you are unsure whether the access being made is Controlled or Supervised, consult with a more experienced Operator, the Crew Chief, or the Duty Assistant **before** selecting an access type.

Remote Key Trees

To facilitate more efficient accesses to experimental areas that are far away from the MCR, some areas at Fermilab have **Remote Key Trees,** located directly outside their respective enclosures**.** Like the MCR key trees, a remote key tree will contain a set of Enter keys for a given enclosure.

The doors to these key trees are secured with a magnetic lock that can be unlocked by turning and holding a BT5 key in the appropriate slot in the MCR. On the right-hand side of the remote key tree, there is a button with a green light that illuminates when the key tree has been unlocked. The person requesting a key will press and hold the button, then pull on the front of the key tree to open it. The key tree remains unlocked for as long as the BT5 key in the MCR remains turned.

Fermilab Test Beam Facility (FTBF) – Controlled Access Leader (CAL) & Their Role

Because the experiments located in the MT6 or MC7 areas at the Fermilab Test Beam Facility (FTBF) change frequently, the experimenters are required to have at least one person trained as a Controlled Access Leader (CAL). The CAL coordinates all aspects of a Controlled Access. They are specifically trained by the FTBF managers to ensure they understand the specific procedures for accessing the enclosures. The CAL is the only person allowed to call the MCR to request a Controlled Access, and to provide the names and ID numbers of the individuals wishing to make the access. The CAL List can be found on the MCR Scratchpad. CALs are not required to be present when a request to go into Open Access is made.

Additional Steps For Issuing Remote Keys

- After receiving a call requesting an access at a remote key tree, verify which area is to be accessed.
    - If the access is at FTBF, as described above, verify the requestor is an authorized CAL using the CAL List.
- Ensure the appropriate enclosure is prepared for access.
- Verify that the access party is at the key tree via the key tree camera on the computer monitor to the right of the Keylogger.
    - Note that the use of the cameras is encouraged in this step, but use of the cameras is not a requirement for issuing remote keys.
- Use the BT5 key to unlock the appropriate remote key tree as described above and inform the requestor they may now open the door.
- Use the above Issuing Keys in the Main Control Room section from step 4 onward.
- Once all requested keys are issued, verify the requestor closes the key tree door.

Remember

- **DO NOT** issue keys for Controlled Access to experimenters at FTBF without an authorized CAL present.
- Monitor individuals and the key issuing process via the remote key tree cameras.
- Inform the Crew Chief **IMMEDIATELY** if access procedures have been violated in any way.
- At least one key must be left in the remote key tree to allow access in an emergency.

Key Types, Exceptions, & Special Permissions

The following sections explain some of the key types that are commonly issued, common restrictions when issuing keys, and access modes for the experimental areas. This is not meant to be a comprehensive listing of the keys and restrictions. If there are any questions regarding the restrictions for a key, do not hesitate to ask a more experienced Operator, Crew Chief, Specialist, Area Manager, or ES&H personnel.

Enclosure Enter Keys

The “Enclosure Enter Keys” are used by Fermilab personnel to allow access to the accelerator and beamline enclosures on site. Some things to keep in mind about Enclosure Enter Keys are:

- Enclosure Enter Keys are interlocked to the enclosure Electrical Safety System (ESS) and may only be issued if the enclosure has been prepared for access.
    - Some enclosures require a written LOTO procedure to be performed by Operators before keys are issued.
- Each person entering an enclosure **MUST** have an Enclosure Enter Key in their possession while in the enclosure.
- At least one Enclosure Enter Key must remain in the key tree.
    - This key is to be used as in the event of an emergency.
    - Some remote key trees have “Emergency Access” listed on the key tag of the last Enclosure Enter Key.

Reset Keys

"Reset Keys" may only be issued to the Operations Department or the Interlocks Group. The Operations Department uses the Reset Keys for the Search & Secure of an enclosure before resuming beam operations. The Interlocks Group uses the Reset Keys for interlock system testing and repair. Most Reset Keys are also interlocked to the enclosure ESS, and they can only be issued if the enclosure has been prepared for access. Reset Keys are **NOT** Enclosure Enter Keys and **DO NOT** allow access to an enclosure on their own. The Keylogger will alert and request confirmation from the issuer when attempting to log out a Reset Key.

Non-Enclosure Keys

"Non-Enclosure Keys" are keys that allow entry to an area that is not interlocked to an Electrical Safety System, but may require training, such as GERT or Radiation Worker training. Be aware of the many Non-Enclosure Keys that are encountered by Operations that have many different rules for issuing. If you're unfamiliar with a key or its rules, stop the key-issuing process and ask.

Shutdown Keys

Many of the major accelerator enclosures are re-cored by ES&H to a Shutdown Core set, instead of the normal HEP Core set. The Shutdown Cores have a greater number of associated keys, allowing a greater number of people to enter the enclosures in order to perform shutdown work and maintenance activities. Some things to keep in mind about Shutdown Keys are:

- Shutdown Keys may allow access to multiple enclosures.
    - Example: A Main Injector Shutdown Key may allow entry to the 8GeV Line Enclosure, MI-10 Enclosure, and MI20-62 Enclosure.
- Shutdown Keys may allow access to enclosure and non-enclosure areas.
    - Example: MI-65 Shutdown Cores are installed in the gate to the elevator, as well as the gate to the MI-65 Enclosure. As a result, the MI-65 Shutdown Key allows access not only to the enclosure, but also to the non-enclosure area at the bottom of the elevator shaft.
- An enclosure may only be re-cored to a Shutdown Core once the area has been prepared for Supervised Access.
- Types of Shutdown Keys
    - Long-Term Shutdown Keys
        - Issuing of Long-term Shutdown Keys are handled by the Operations Duty Assistant.
        - Personnel who are issued Long-term Shutdown Keys keep that key for the duration of the shutdown, and they do not need to return the key at the end of the workday.
    - Daily Shutdown Keys
        - Issued like a normal Enclosure Key from the MCR.
        - Must be returned to the MCR at the end of the workday.
- See *ADDP-OP-0410 Enclosure Core & Key Swap Procedure* for more information on Shutdown keys.

Open Access

Open Access is a form of access to an experimental enclosure where the interlocks to the enclosure have been dropped, doors may be propped open, and personnel may enter and leave the enclosure without the need for keys. Open Access is allowed only for **specific** enclosures, such as MT6-1, MT6-2, MC1, and MC7: **Just because an enclosure has had its interlocks dropped does NOT necessarily mean that the enclosure is in Open Access.**

- Upon request from the experimenters to go into Open Access, Operators shall verify the validity of the request and follow the Remote Key Tree key issuing procedure.
- For MT6-1, MT6-2, and MC1:
  - The requestor may remove an Enclosure Enter Key to open the enclosure entrance and drop the interlocks without checking out the key. They must then immediately return the key to the key tree and close the key tree door.
  - You must remain on the phone line with the experimenter and monitor them via the key tree camera during this process to ensure the key is returned.
- For MC7:
  - It is impractical to remain on the line with experimenters at MC7, since the enclosure door is not in the immediate vicinity of the key tree. In this case, the key must be logged out to the experimenter using the Remote Key Tree key issuing procedure as normal. They will use the key to drop the interlocks and call back to return it later.
- NM4 is no longer able to go into Open Access in the era of SpinQuest. The only modes of access for NM4 are now Controlled and Supervised.

Area Restrictions and Special Alerts

The Keylogger does not have a mechanism in place to automatically observe some temporary area restrictions. Due to the ever-changing nature of these restrictions, it is necessary for the Operators and Crew Chiefs to ensure they are observed.

- Special Work
  - On occasion, some work activities may require further restricting access to an area until that work is complete.
  - Example: The Interlocks Group are the only personnel allowed in an enclosure during testing of the Interlock System due to the nature of this work.
- Authorized-Access Lists
  - Some areas maintain a permanent list of authorized entrants. When issuing a key to these areas, a pop-up box (*Figure 7*) may appear **prior** to the training qualification check, indicating the person is not on the authorized access list. Hover the cursor over the key number to display the access list for that key.
  - In general, keys with Authorized Access Lists should only be issued to people who are on the list.

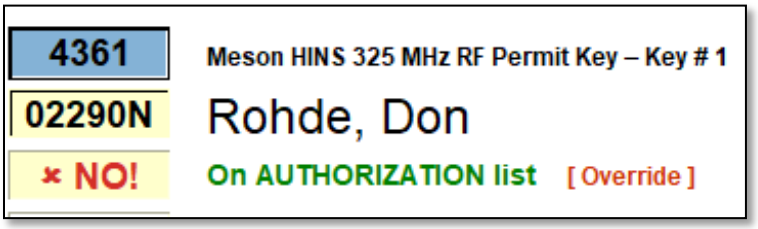

Figure 7

- Alert Messages
  - Any key may be assigned one or more Alert Messages which will be displayed whenever that key is logged out, regardless of the borrower's qualifications. Below is an example of a *typical* alert message but there are many others.

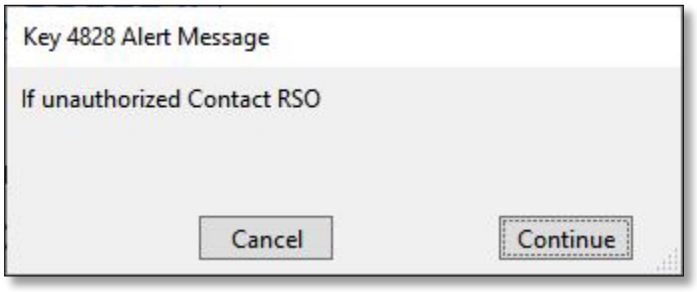

Figure 8

- Area Coordinator Restrictions
  - An Area Coordinator may impose access restrictions to their area at their discretion. Usually, the purpose is to limit access to personnel who are actively participating in work.
  - These restrictions remain in place until rescinded by the Area Coordinator.

Non-Fermilab Personnel Escort into Enclosures

At times, it may be necessary to issue a key to a person who is not an employee, contractor, or user of Fermilab (e.g. they have no ID number). The typical reason for this is when a VIP tour is scheduled. **The tour and authorization to issue the key to non-Fermilab personnel must be approved by ES&H in advance.** The Keylogger has a feature to handle this, however it is preferred, in this circumstance, to let the Operations Duty Assistant handle the issuing of keys.

If the Operations Duty Assistant (Key Admin) is not available:

- The first key issued to the group must be to the Fermilab employee who will escort the tour, individual or group, using the "Issuing Keys in the Main Control Room" procedure, above. As such, the escort must have all of the proper training in order to obtain the first key.
- The subsequent keys are issued by entering the Key Barcode number and then clicking on the green "Escorted Personnel" button below where the ID number was entered.
- After pressing the "Escorted Personnel" button, the issuer will be given a text box to enter the name of the person being issued the key and the escort's ID number. (*Figure 9*)

If you are unsure of a restriction, status of an enclosure, prompts being displayed by the Keylogger, or any request made by a key requestor, do not hesitate to stop and ask more experienced Operators, Crew Chiefs, or Experts.

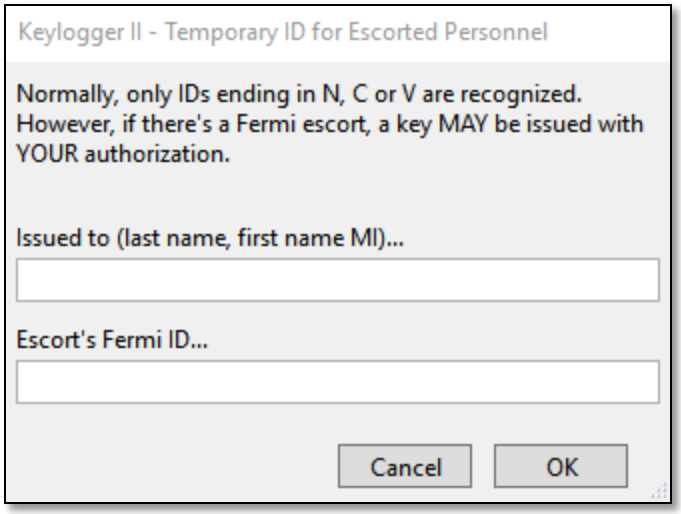

Figure 9

Troubleshooting & Tips

- Shortcut to enter a Contractor's ID Number
  - When entering an ID Number for a Contractor, one that ends in "C", you can type the number and press the period key on the number pad to append the "C" to the number & enter.
- Multiple keys to the same ID
  - Use the + key on the keypad to quickly populate the ID box with the ID Number of the last person who was issued a key.
- Correcting an ID Number or Key Barcode Number in a completed transaction
  - If the incorrect ID Number or Key Barcode Number was entered during the key transaction, simply log the key back in within one minute, and redo the transaction with the correct information. The Keylogger will not save the occurrence of transactions that last less than one minute.
  - The Duty Assistant can undo older transactions, but they remain recorded.
- There is a "Last Name Lookup" button if an ID Number is unknown or not provided.
- Changing the Enclosure Access Mode
  - In the event a key is logged out and the incorrect access mode was selected (Controlled Access instead of Supervised Access for example) the mode can be changed by clicking the key that was issued in the "Outstanding Keys" table, and then clicking the "CA to SA" button (*Figure 10*). Once all the keys for an enclosure are returned, the access type is changed to CA automatically.

Figure 10

- Starting the Keylogger Program
  - To start the Keylogger program, double-click on the “Keylogger II shortcut” usually in the upper left corner of the computer’s desktop.

Logging In a Key

To log in a returned key, type the key barcode number into the “Key” box on the top window of the Keylogger and press enter. The key listing will be removed from the Outstanding Keys list and moved to the Completed Transactions Log.