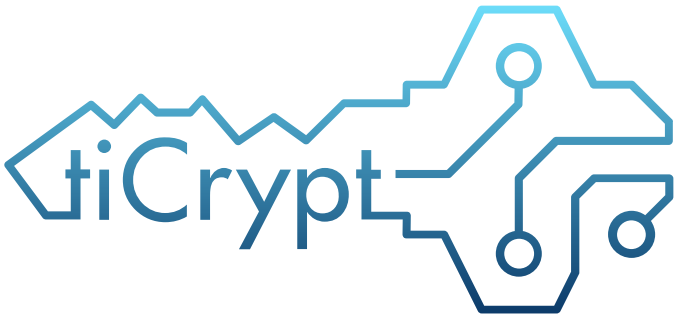


Site Key and Escrow

Take Control Of Your Data

Tiffany Dixon

Tera Insights, LLC

Contents

1 Overview

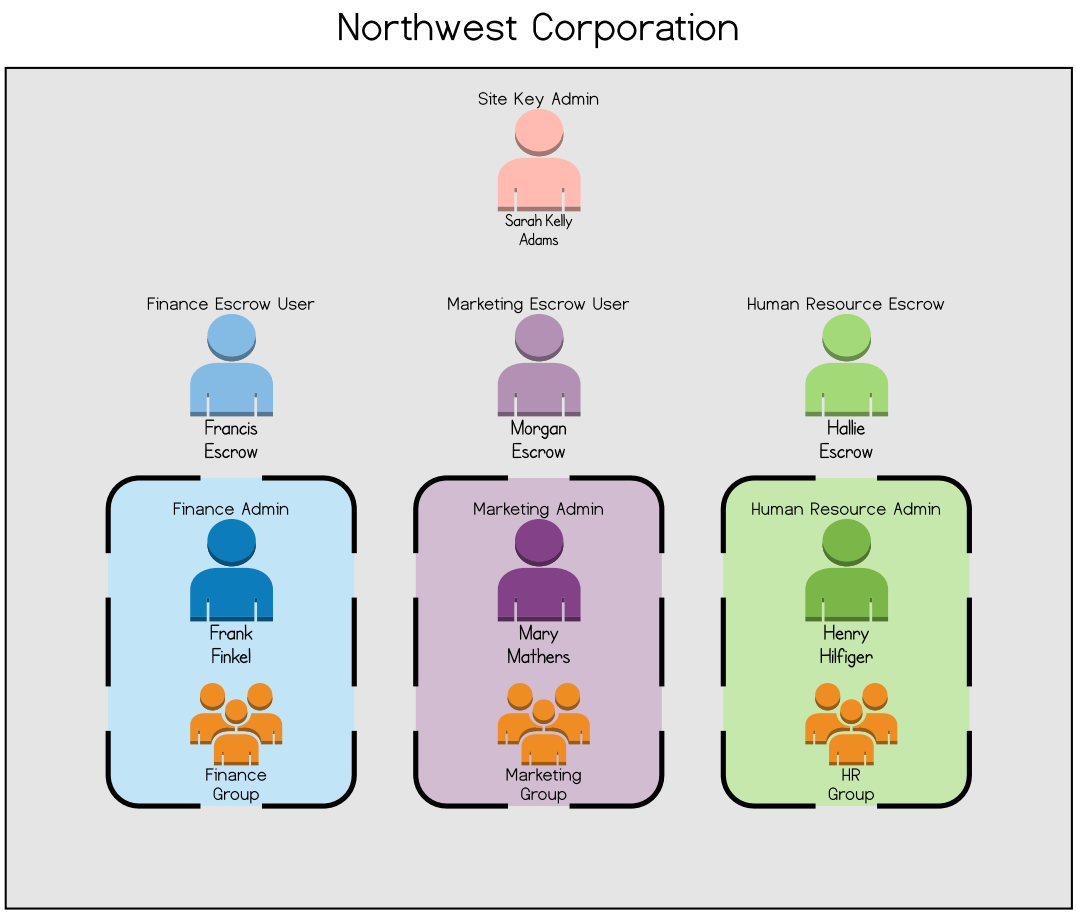
1.1 The Philosophy

The roles of site key administators and escrow users play an essential part in the structure of *tiCrypt* . The purposes of each role will be described using the example below. Much with most things in *tiCrypt* , these roles are meant to act as a distribution of power throughout the system.

Site Key Administrator This role is meant to be used for offline certification of escrow groups and escrow users. This user should not be a normal system administrator or an escrow user. In the above example, this user would be Sarah Kelly Adams.

Escrow Users These users are responsible for recovering lost private keys for normal *tiCrypt* users. These users should not be administators and should be used only for key recovery purposes.

System Administrators These users are the admins and super admins in *tiCrypt* . These users are responsible for regular user management throughout the system and should have a complete understanding of the users within their department or team. These users are responsible for activating new users, managing user groups, and monitoring activity for their respective group.



As seen from the above example, the escrow users and site key administrators should be independent from individual departments or teams. However, these users have a very important interaction with normal users of *tiCrypt* and play a big role in the security of the system.

2 Site Key and Certificates

This chapter is only for Sitekey administrators. Super Admins and Admins will not have access to the site key interface or be able to digitally sign certificates. In order to use the sitekey and certificate interface, the site key must be counter-signed by the Tera Insights key and placed in the correct configuration file. This site key is used to sign certificates that will get passed into *tiCrypt* .

The sitekey interface is designed to be an offline tool that enforces digital signitures and prevents these signitures from being forged.

2.1 Creating a Sitekey

To navigate to the site key creation page, select the **escrow user** link on the main *tiCrypt* login page, and then select **create site key** on the escrow login page. This link will redirect to a registration page that looks very similar to the *tiCrypt* user registration page. On this page, the public-private site key pair is created, a password to encrypt the private key is required, and terms are listed that must be accepted. The last step is saving the private key.

In order to start using this site key, the public part of the key will have to be digitially signed by Tera Insights and will then be stored on the server. This operation is performed in the initial setup of the system. However, until this occurs, the site key cannot be used to sign any certificates.

Saving your encrypted private key

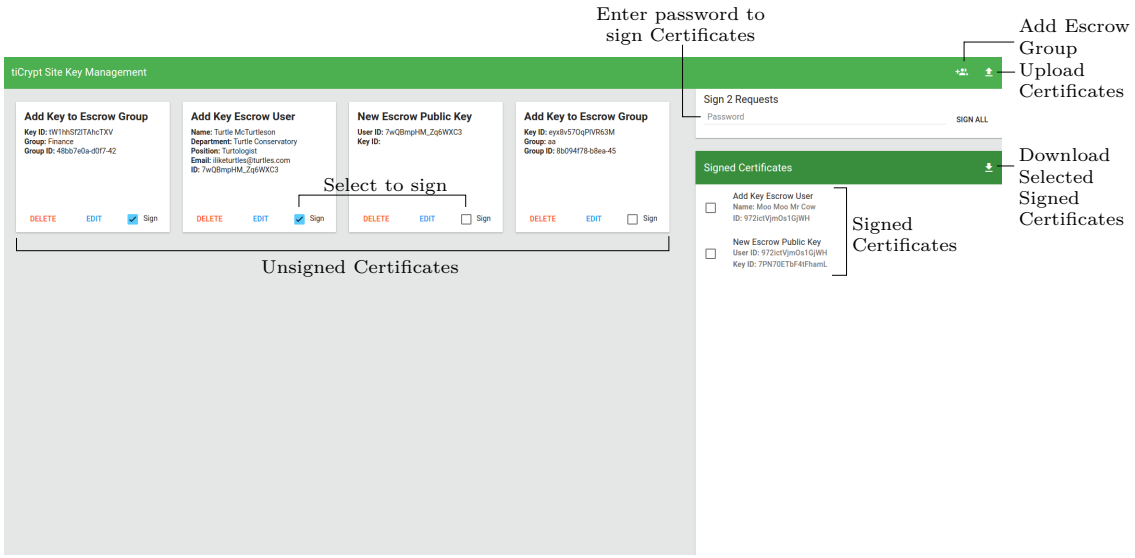
This private key is not recoverable after leaving the registration page and should be stored accordingly. Some tips on storing your private key include storing it on:

- **Recommended** A USB Drive (prevents from data loss on a local computer and allows for use of *tiCrypt* on multiple computers and browsers)
- The local computer you will be accessing *tiCrypt* on, in an appropriately named folder and location

2.2 Role of the site key administator

An important concept in the *tiCrypt* architecture is the idea of separation of powers. A site key administator's role is to digitally sign certificates made by *tiCrypt* escrow user requests. The site key administrator does not create certificates, and cannot upload signed certificates into the *tiCrypt* system. The sitekey admin system is offline, and therefore has no interaction with system servers.

Both site key administators and normal administrators rely on each other, but both have different abilities in the system to avoid a single user having too much power or responsibility.



2.3 Uploading Unsigned Certificates

Uploading a certificate is done by selecting the icon in the top-right corner of the interface OR dragging and dropping one or several certificates onto the interface from your file system.This action will open up your local file system, where certificates can then be selected.

At this point, the only certificates that the site key administrator should be uploading are **Escrow User Requests**. Once the certificates have been successfully uploaded, they are now ready to be signed.

2.4 Editing and Signing Certificates

Editing Certificates

Notice an issue in a certificate or wish to change information associated with the certificate? Once the certificate has been uploaded, it will have the an **edit** option. The editing options will depend on the certificate, but once satisfied with the changes, you can be save them before they are signed.

Signing Certificates

On each certificate, there is a checkbox to select that you wish to sign this certificate. Therefore, by checking multiple certificates, you may sign more than one certificate at a time. To sign with the site key, the password to decrypt it is required. Once the password has been entered, select **sign**.

All signed certificates will then appear in the **Signed Certificates** panel.

Exporting Signed Certificates

To export signed certificates, select the  icon in the signed certificates panel. This will download all of the signed certificates onto your local machine where they can then be shared with system admins to be added to *tiCrypt* .

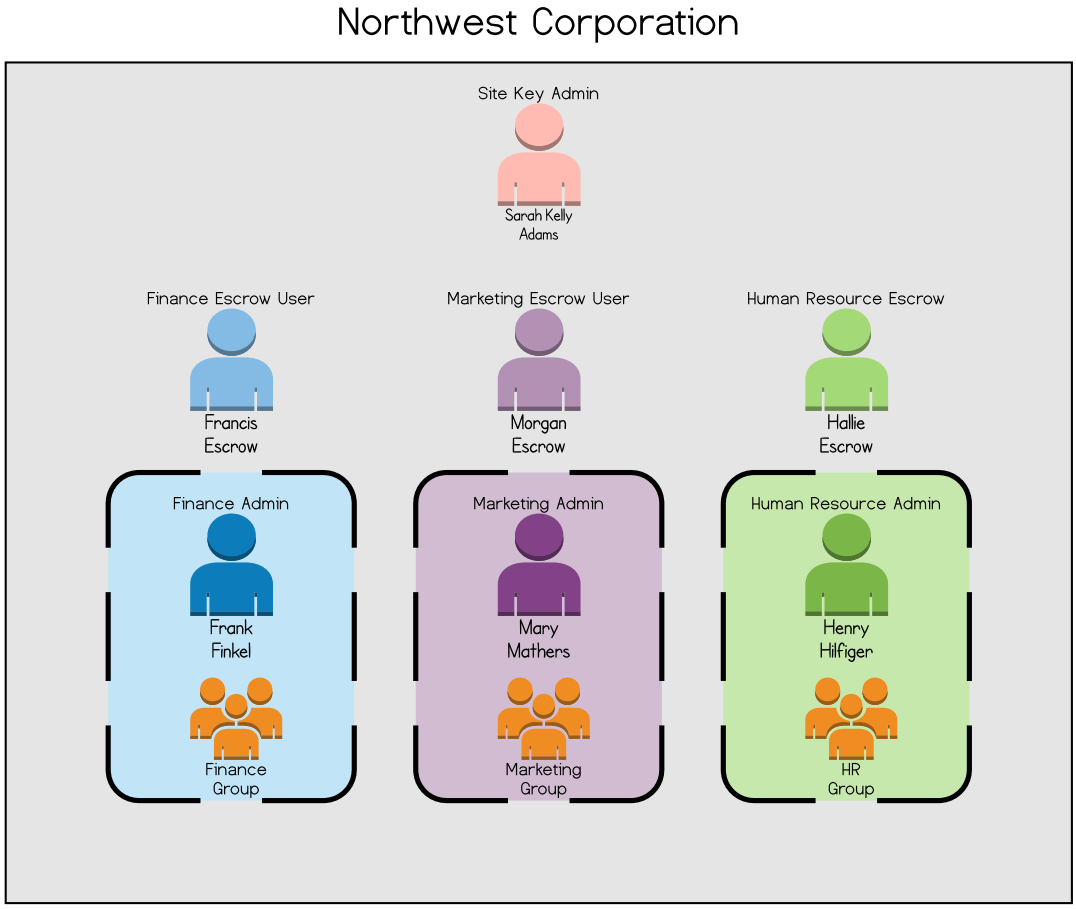
Transferring signed certificates to system administrators is left up to preference of the site key admin. There is no built in system of transferring these certificates.

2.5 Escrow Groups

One of the site key administrator abilities/responsibilites is creating new escrow groups. To do so, select the  icon located in the top-right corner of the interface. Generally, escrow groups are created in accordance with each department of a company/university/business. For example, escrow groups might be Finance, IT, Marketing, Human Resources, etc. These groups are meant to mimic the teams/groups of an organization to allow for familiar workflows.

2.5.1 Editing Escrow Groups

2.6 A Full Example



Suppose, for example, the Northwest Corporation is incorporating *tiCrypt* into their current system. The first step in this process is creating a **Site Key**, which will be done by Sarah Kelly Adams, the chosen Site Key Administrator. Once the site key is digitially signed by the Tera Insights Key and stored on the server, Sarah can then start signing certificates.

Along with creating the site key, Sarah Kelly Adams will also be responsible for the initial setup of the Escrow Groups including

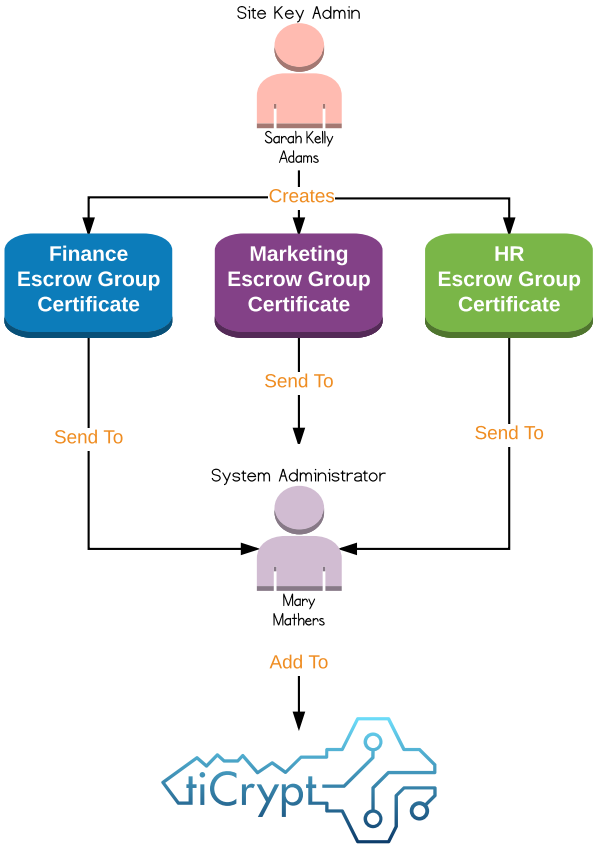
- Finance,
- Marketing, and
- Human Resources

These escrow groups will be responsible to recovering the lost keys of their respective departments. In the above example, Francis Escrow is the Finance Escrow user, Morgan Escrow is the Marketing Escrow user, and Hallie is the Human Resources Escrow user. These users are not actually

members in these groups, but act as an outside resource for this key recovery mechanism.

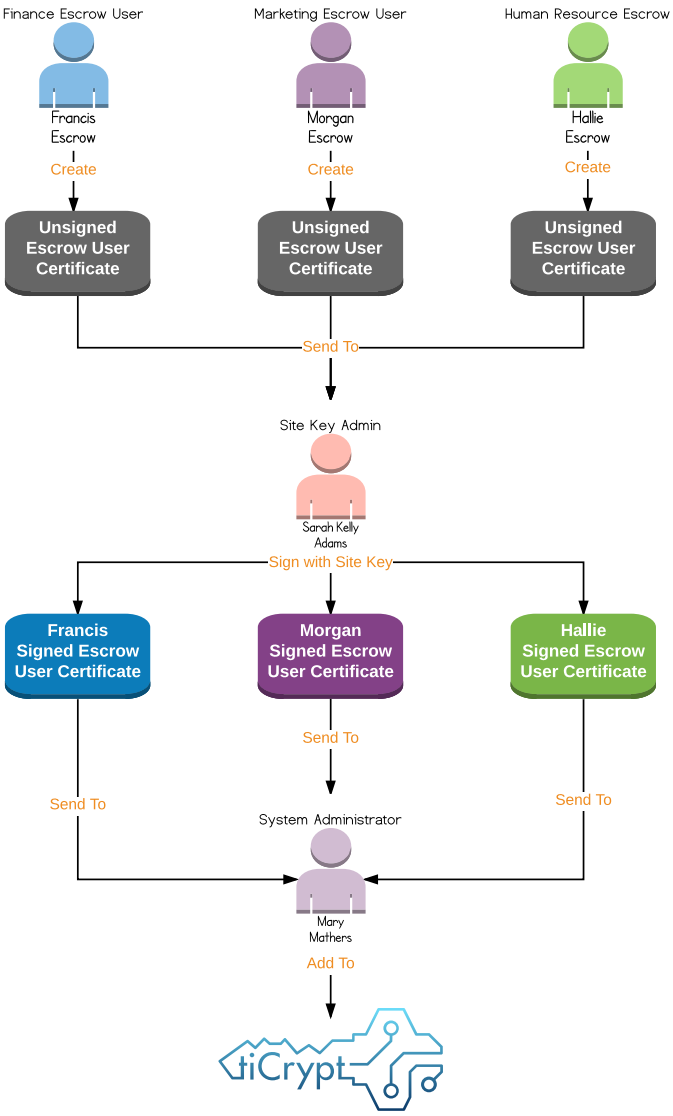
The process proceeds as follows:

1. Sarah will generate 3 escrow group certificates including the finance, marketing, and hr escrow groups.
2. Sarah will sign these new escrow group certificates with the site key.
3. Sarah will download the newly signed certificates onto her local machine and email them to Mary, a *tiCrypt* system administator
4. Mary will add them to *tiCrypt* using the certificate Management tools (see **Admin Manual** for more information)



Keep in mind, in this example we use Mary Mathers, but these certificates may be sent to any system administator including Frank Finkel and Henry Hilfiger.

The next step is to **add Escrow Users to these groups**.



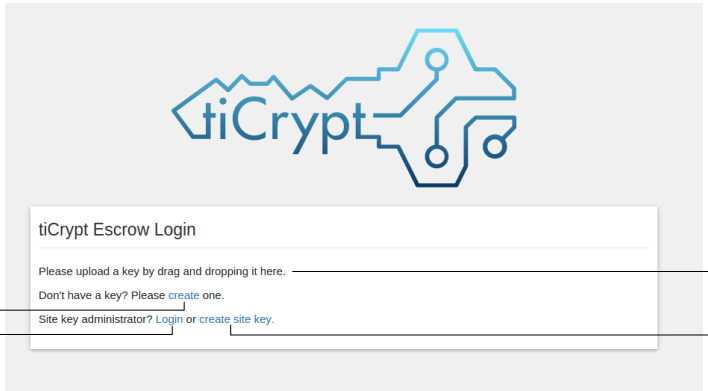
The process proceeds as follows:

1. Francis, Morgan, and Hallie will register to become escrow users using the Escrow Registration page (see **Key Escrow**)
2. Francis, Morgan, and Hallie will send their unsigned certificates to Sarah
3. Sarah will assign Frances, Morgan, and Hallie to escrow groups and sign the certificates
4. Sarah will send the newly signed certificates to Mary
5. Mary will add the signed certificates to *tiCrypt* . For more on adding certificates into *tiCrypt* , see the **Admin Manual**

3 Key Escrow

Key Escrow is tiCrypt's way of protecting the recovery process of lost keys in the system. It works by essentially splitting up a user private key cryptographically into a specified number of parts and sending the peices to different escrow users. The default number of parts is 3, so this is the example value we will use to describe the system. Once the key is split up, the 3 pieces of the key are given to 3 different escrow groups, so each escrow group has a different part. Escrow users in tiCrypt are separated by groups, and groups may only receive 1 part of the escrowed key. This is done to avoid collaboration and malicious behavior between users of the same group.

3.1 Escrow Key Creation



To navigate to the key creation page, select **escrow user** on the main login page.

Once on the escrow login page, select **create** to naviate to the registration page.

The registration page will generate the escrow keypair, then ask for some information from the user including an email, name, department, position, and password that will protect the escrow keypair.

Once all this information is filled out, the option to download the escrow private key and certificate request will be available. Store these just as you would the private key for a tiCrypt user account. For this escrow key to be usable, the certificate must be digitally signed by the sitewide admin with the sitekey.

3.1.1 Submitting the certificate for approval

To begin using the escrow account, the site key administrator must assign the escrow user to an escrow group and then digitially sign the certificate. (see **Site Key** for more information). There is no submission process available

through *tiCrypt* , so the user can decide how they would like to send the unsigned certificates to the site key admin.

3.2 Escrow Login

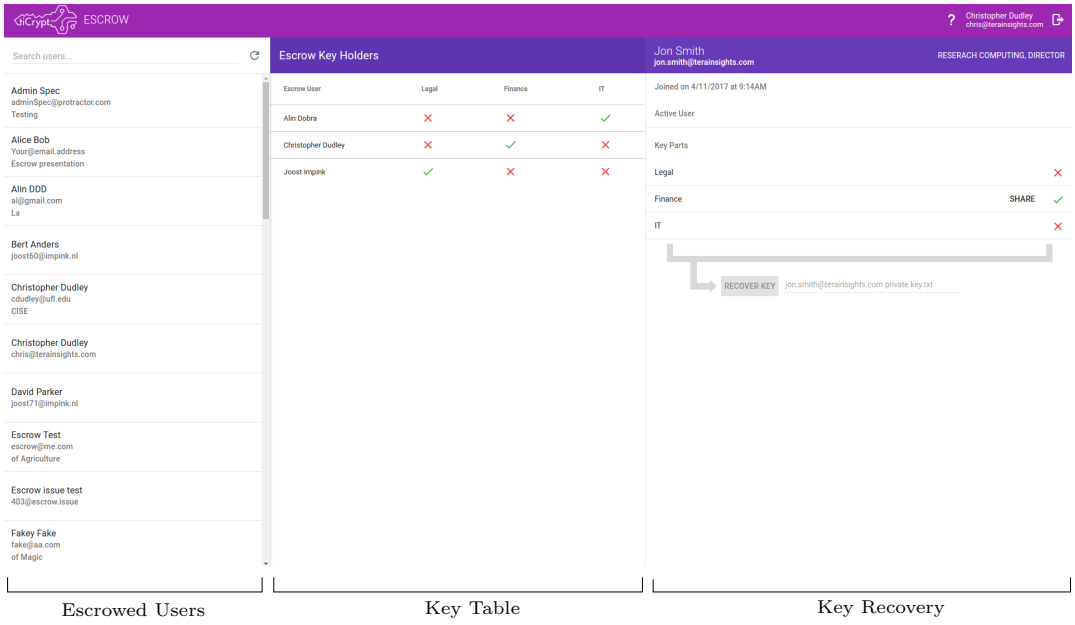
To navigate to the escrow login page, select **escrow user** on the main login page.

Once on this login page, drap-and-drop your escrow key onto the web-page. When it has successfully uploaded, you will be prompted for the password protecting the key. Once that information is filled out correctly, select **Login** to enter the escrow system.

Note: The escrow user certificate must be signed and submitted in order for an escrow user to login to the escrow system.

3.3 Escrow System Interface

The escrow interface is divided into 3 different panels, including Escrowed Users, Escrow Key Table, and Key Recovery.



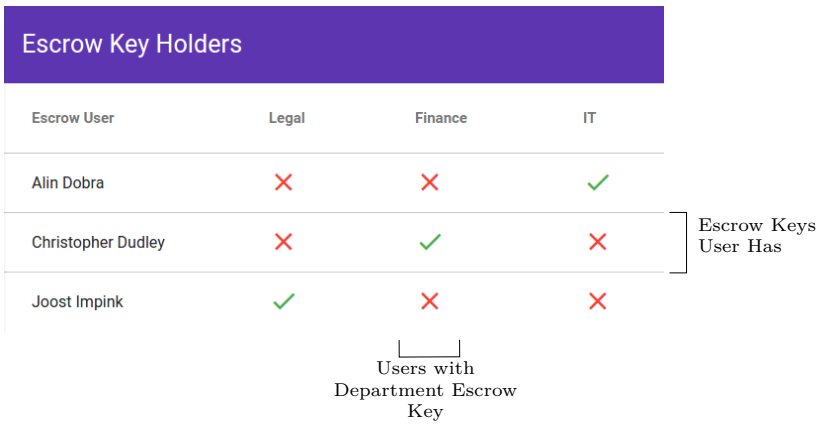
3.3.1 Escrowed Users

All users whose private keys have been escrowed will be listed here. For instructions on how to escrow a user key, See **Admin Manual**.

3.3.2 Escrow Key Table

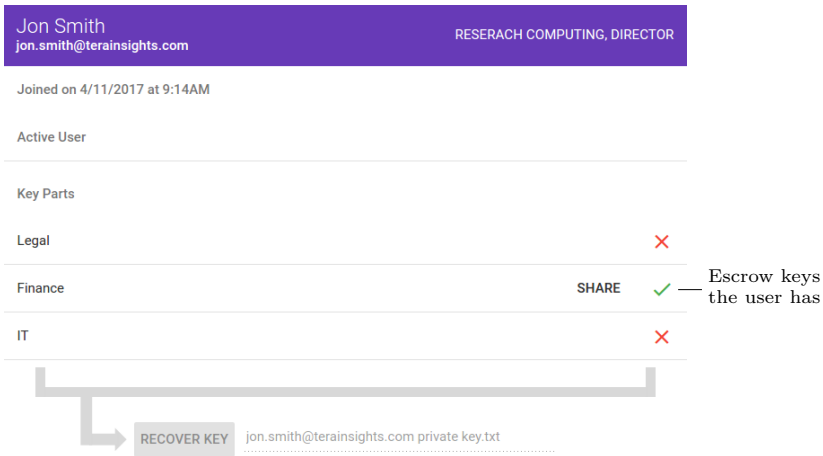
The Escrow Key Table shows the escrow users and the escrow keys they possess. The rows of the table represent the keys that one user has. The columns of the table represent the users that possess keys per escrow group.

In the example below, Christopher possesses only the Finance group key (as seen from the rows), and he is the only user who has the escrow key for the Finance group (from the columns).



3.3.3 Sharing Key Parts

An escrow user can share any keys they possess, whether it is from their group or it was shared with them by another escrow user. To share a key with another escrow user, select the **SHARE** option next to the key part and select the escrow user you wish to share they key part with.



Once an escrow user has all the key parts, the user key can be recovered and downloaded.

3.4 Key Recovery

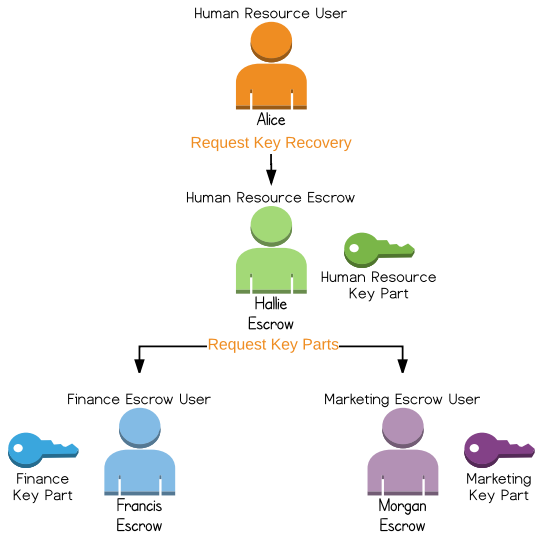
Once an escrow user possesses all of the key parts for a user key, the user private key can be recovered and downloaded. This escrow user will then be responsible for giving the *tiCrypt* user their recovered private key.

3.5 A Full Example

Suppose a *tiCrypt* user, Alice, loses her private key and needs to recover it. The process will look like such:

1. Alice will request a key recovery from her department escrow user (Hallie in this case)

2. Hallie will request the other key parts needed from the Finance and Marking Escrow teams. (This is done independently of the system)



3. Once Hallie has all the key parts, she will recover Alice's private key.

4. Hallie will send Alice her recovered private key. (This is also done independently of the system)