



UBS KeyLink Site Restriction Management Summary

Version: 1.0. / 01.05.04

I. Contents

1.	What is Site Restriction?	1
1.1	What is Site Restriction?	1
1.2	Risks and Considerations.....	1
1.3	How does Site Restriction work, practically?	2
1.4	How does Site Restriction work, technically?	3
1.5	Contract (documentation).....	4

1. What is Site Restriction?

1.1 What is Site Restriction?

Some customers need to be able to document and control their electronic banking operations more precisely than others.

With our Site Restriction feature, we offer the possibility to limit access to UBS KeyLink to certain computer stations only. A user will only be able to use the UBS KeyLink service when accessing from a UBS KeyLink authorized work station.

Site Restriction is an **optional** feature, only enabled on the customer's request and can be set for single users, groups of users or the entire relationship.

1.2 Risks and Considerations

A user with the privilege to unlock workstations can unlock any workstation he desires. Whether the workstation is trustworthy enough to unlock is entirely determined by the Administrative User designated by the Customer.

There is no audit trail to track who and when a workstation has been unlocked.

1.3 How does Site Restriction work, practically?

In UBS KeyLink there are three possible types of users: Administrative Users, Restricted Users and Unrestricted Users.

Administrative User

First choose an "Administrative User". This is the person who is authorized to enable or disable the machines from which UBS KeyLink can be accessed.

When the Administrative User logs into UBS KeyLink from a workstation, he may enable or disable that machine for all users.

To set this privilege, the Administrative User must go to a user dialog in the menu 'Tools' → 'Site Restriction'. This will give the possibility to enable and disable the workstation for Site Restriction, which results in creating a token and saving it in the java.home directory. The java.home directory has been chosen because this directory is user independent. Write permission in java.home directory is needed to generate the token.

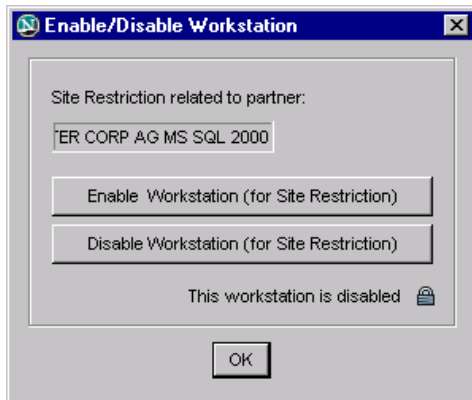


Fig: Enable/Disable Site Restriction Dialog

If the Administrative User enables a workstation for Site Restriction a token is created. Otherwise, if a workstation is disabled again, the token will be deleted.

The token is machine dependent and cannot be transferred to another machine and can only be generated by the Administrative User.

Restricted User

Restricted Users may only access UBS KeyLink from machines defined by an Administrative User.

Unrestricted User

Unrestricted Users may access UBS KeyLink from any machine. Site Restriction is set on a group level, so unrestricted users are generally for those customers who don't choose the Site Restriction option.

When Site Restriction is set up for a user in a group, the following will happen:

- User authenticates himself to UBS KeyLink in the usual way, login and password
- If the customer is marked as 'Site Restricted', UBS KeyLink will look for a machine and customer specific token on the machine the login request is made from. Access will only be granted if a valid token can be found on the user's machine

1.4 How does Site Restriction work, technically?

The client uses a token to check if a user has the privilege to login from the computer he is working at. This token contains the hard-disk serial number (HD SN) and the partner. The token will be created on the server and saved on the client-side.

During login (beside login-name and password) the token and the HD SN will be sent to the Paris Service. The Paris Service creates a new token with the given Partner and HD SN. Now the service compares the new created token with the one sent by the client. If this comparison matches the login is successful.

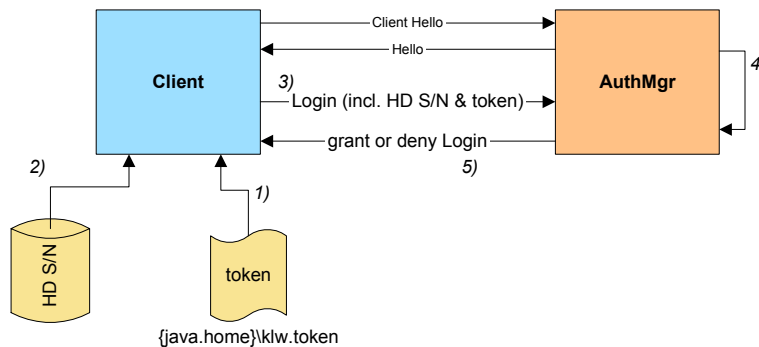


Fig: How login with a token works

1. Read the token from file
2. Read HD SN (if a token exists)
3. Send the login message including the token and HD SN to the server
4. Create a new token and compare it with the token sent by the client
5. Grant or deny login

If no token exists on the client-side a zero token will be sent with the login message.

A token is a hardware-bound key. It is needed to identify the workstation where UBS KeyLink has been started as well as make a relation to the partner the user belongs to. Using the partner as a parameter for the token has the advantage that only users belonging to the same partner have access to an unlocked workstation.

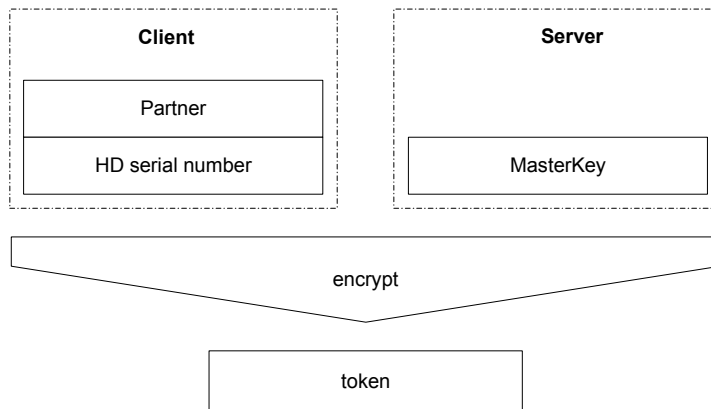


Fig: Token structure

1.5 Contract (documentation)

Site Restriction will be documented on a User level within our contract structure. Therefore, selections will be made on the UBS KeyLink Authorized User Registration Form.

If you do not want the Site Restriction option, all users should be marked as “Unrestricted User”.

If you do want the Site Restriction option, choose one “Administrative User” to log in to the desired machines and enable them with a token. All other users should be marked as “Restricted Users.”