**How to create a User Delegation SAS using Azure CLI ?**

Below 2 steps are used to create a User Delegation SAS using Azure CLI

**1. Assign permission with Azure RBAC —**

The following example assigns the Storage Blob Data Contributor role, which includes the **Microsoft.Storage/storageAccounts/blobServices/generateUserDelegationKey** action. The role is scoped at the level of the storage account.

Replace placeholder values in *angle brackets* with your own values -

az role assignment create \  
 --role "Storage Blob Data Contributor" \  
 --assignee <email> \  
 --scope "/subscriptions/<subscription>/resourceGroups/<resource-group>/providers/Microsoft.Storage/storageAccounts/<storage-account>"

For more information about the built-in roles that include the **Microsoft.Storage/storageAccounts/blobServices/generateUserDelegationKey**action, see [Azure built-in roles](https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles).

Now the assignee is ready to generate an User Delegated SAS Token.

**2. Create a user delegation SAS for a container -**

The following example returns a user delegation SAS token for a container. Remember to replace the placeholder *values in brackets* with your own values:

az storage container generate-sas \  
 --account-name <storage-account> \  
 --name <container> \  
 --permissions acdlrw \  
 --expiry <date-time> \  
 --auth-mode login \  
 --as-user

*When creating a user delegation SAS, the --auth-mode login and --as-user parameters are required.*

*Specify*login*for the --auth-mode parameter so that requests made to Azure Storage are authorized with your Azure AD credentials.*

*Specify the --as-user parameter to indicate that the SAS returned should be a user delegation SAS.*

***Note — When you create a user delegation SAS with the Azure CLI, the user delegation key that is used to sign the SAS is created for you implicitly.***

Supported permissions for a user delegation SAS on a container include Add, Create, Delete, List, Read, and Write. Permissions can be specified singly or combined. For more information about these permissions, see [Create a user delegation SAS](https://docs.microsoft.com/en-us/rest/api/storageservices/create-user-delegation-sas#specify-permissions).

**What are the best practices while using SAS?**

✓ Managing SAS can sometimes becomes a nightmare. One of the best solution is to create an application/middleware that can authenticate external users and allow them to request SAS for a specific operation on a specific container or file & provide SAS for consumption.

✓ Always use HTTPS to create or distribute a SAS. If a SAS is passed over HTTP and intercepted, an attacker performing a man-in-the-middle attack is able to read the SAS.

✓ If you set the start time for a SAS to the current time, failures might occur intermittently for the first few minutes due to clock skew. In general, it is suggested to set the start time to be at least 15 minutes in the past.

✓ Make sure you are prepared if a SAS is compromised. Have a revocation plan in place for a SAS.