|  |  |
| --- | --- |
| SAS | Account key |
| A shared access signature is a signed URI that points to one or more storage resources. |  |
| The URI includes a token that contains a special set of query parameters. The token indicates how the resources may be accessed by the client. |  |
| One of the query parameters, the signature, is constructed from the SAS parameters and signed with the key that was used to create the SAS. This signature is used by Azure Storage to authorize access to the storage resource. |  |
| **SAS signature and authorization**  You can sign a SAS token with a user delegation key or with a storage account key (Shared Key). |  |
|  |  |
|  |  |
|  |  |

| **Type of SAS** | **Type of authorization** |
| --- | --- |
| User delegation SAS (Blob storage only) | Azure AD |
| Service SAS | Shared Key |
| Account SAS | Shared Key |

[Q58. How to create a Storage Account? (vkinfotek.com)](https://vkinfotek.com/azureqa/how-to-create-a-storage-account.html)

portal.azure.com

* Authentication method: Access key

Microsoft recommends that you use Azure AD credentials when possible as a security best practice, rather than using the account key, which can be more easily compromised. When your application design requires shared access signatures for access to Blob storage, use Azure AD credentials to create a user delegation SAS when possible for superior security.

**USER DELEGATION SAS vs ACCOUNT SAS**

Text, table

Description automatically generated with medium confidence

Timeline

Description automatically generated with low confidence

**How is User delegation SAS created?**

1. User logins in with Azure AD credentials.
2. On successful Authentication, an OAuth token is returned.
3. This token is used to request a user delegation key.
4. User delegation key is used then to create a user delegation SAS token
5. This SAS token can be used in a query param to request Azure storage resources based on permissions the user has.

|  |  |
| --- | --- |
| User Delegation SAS | Account SAS |
| To create a user delegation SAS, you must first request a user delegation key, which is then used to sign the SAS. |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

User delegation SAS is secured with Azure AD credentials instead of storage account keys. This prevents clients/applications from storing/retrieving storage keys to create SAS.

Clients retrieve a user delegation key tied to their Azure Active Directory (AD) account and then use it to create SAS tokens granting a subset of their own access rights. User delegation SAS tokens are now supported for use with production workloads and are available in all clouds and all regions of Azure.

**User delegation SAS**

1. When a client accesses storage resources using a user delegation SAS, the request to Azure storage is first authorized with Azure AD credentials that were used to create the SAS.
2. The RBAC (role-based access control) permissions granted for that Azure AD account, together with the permissions explicitly granted on the SAS, determine the client's access to the resource.
3. The effective permissions are an intersection of the permissions granted to the security principal and the permissions granted on the SAS resource.

The biggest advantage of using a user delegation SAS is that you don't need to store the account access key in your code. This makes it a highly preferred approach for securing access to Azure AD.