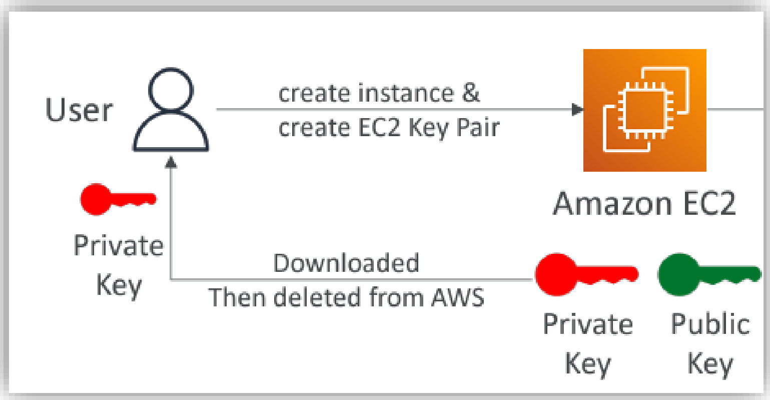
EC2 Key Pairs

AWS Certified Security Specialty SCS-C02

EC2 Key Pairs are essential for securing access to Amazon EC2 instances via SSH.
They consist of a private key and a public key, each serving a distinct purpose in ensuring secure communication.

When you create a key pair in AWS, the private key is downloaded to your machine, AWS deletes the private key from its servers immediately after this.



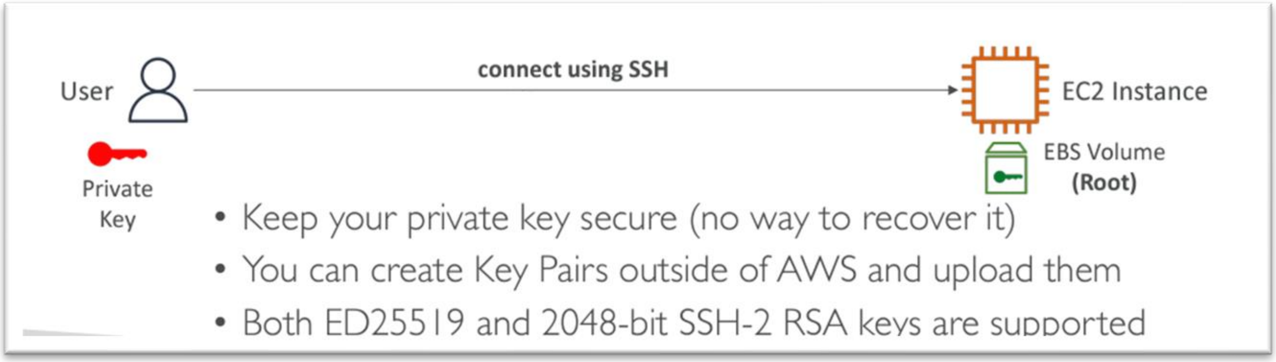
Private Key: This key is securely downloaded to your local machine. AWS does not retain a copy of the private key once it's downloaded, ensuring that only you have access to it.

Public Key: AWS stores this key and uses it to verify that SSH connections are authorized.

We can create Key Pairs using external tools and then upload the public key to AWS. This allows for control over the key creation process.

SSH Connection Process

When we attempt to connect to our EC2 instance via SSH, the protocol uses your private key, The instance verifies this private key against the public key stored in the authorized_keys file If they match, the instance allows the SSH connection. So, the idea is that our private key must be kept secure.



- Keep your private key secure (no way to recover it)
- You can create Key Pairs outside of AWS and upload them
- Both ED25519 and 2048-bit SSH-2 RSA keys are supported

Note:

When we delete a Key Pair from the EC2 console, the Key Pair is removed from the console and is no longer listed there. However, this action does not affect the EC2 instances that were launched using that Key Pair. The associated public key remains on these instances, stored in the authorized_keys file. Therefore, deleting the Key Pair in the console does not directly impact access to the existing instances or remove the public key from them. To manage access properly after deleting a Key Pair, we may need to manually update or remove the public key from the instances if necessary, or generate a new Key Pair and update the instances with the new public key. This ensures continued secure access and aligns with our current security practices.

Automating Key Management

Use the SSM Run Command utility to automate the addition and removal of public keys on EC2 instances. This is useful for managing large environments.

In conclusion

EC2 Key Pairs, based on RSA encryption, are essential for secure SSH access to EC2 instances. The private key is downloaded and stored securely on your machine, while AWS retains only the public key. Proper management of these keys is crucial: deleting a Key Pair from AWS only affects its listing, not the instances themselves. Automating key management with tools like SSM can streamline access control in larger environments.