1. Identity Issuer (University): In this example, let's assume a university is the identity issuer. The university issues verifiable credentials to its students, such as academic degrees or certificates.
2. Generating the Verifiable Credential: When the university issues a verifiable credential to a student, it includes the student's relevant information, such as their name, degree, and graduation date. The verifiable credential is created using a digital signature generated by the university's private key. This signature ensures the integrity and authenticity of the credential.
3. Decentralized Identifier (DID): The student, as the DID subject, has their own decentralized identifier (DID). The DID is associated with their public key and is under their control. The student can use this DID to receive and manage verifiable credentials.
4. DID Document: The student, as the DID subject and controller, creates a DID document that contains their public key information. The university's public key, or the public key of the specific department responsible for issuing the credential, can be included in the DID document.
5. Verifying the Verifiable Credential: When the student presents their verifiable credential to a verifier, such as a potential employer, the verifier follows these steps to verify the public key:
6. a. Resolve the DID: The verifier resolves the student's DID to retrieve the associated DID document.
7. b. Validate the DID Document: The verifier validates the integrity and authenticity of the DID document. This can involve checking the digital signature or verifying the consistency of the document using a trusted decentralized identifier resolution mechanism.
8. c. Extract the Public Key: Once the DID document is validated, the verifier extracts the public key associated with the university or the issuing department.

9. d. Verify the Digital Signature: The verifier uses the extracted public key to verify the digital signature on the verifiable credential presented by the student. By confirming that the digital signature matches the public key, the verifier can ensure that the credential hasn't been tampered with and that it was issued by the university or the authorized department.
10. Through this process, the verifier can trust the authenticity and integrity of the verifiable credential presented by the student without relying on a centralized authority or directly contacting the university.