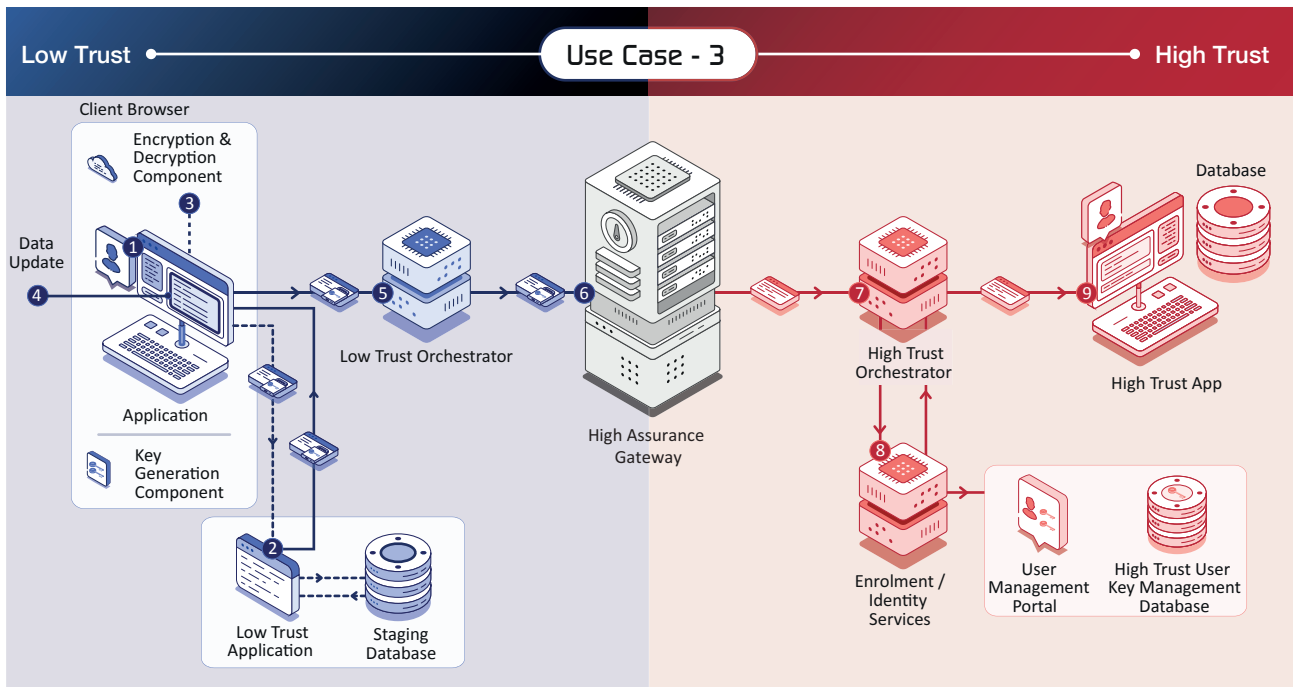# Use Case 3

Data securely collected and processed at low trust, then transferred to high trust for additional processing and fortified storage.

Application Needs

- Application has high volume transactions and needs to store the staging data at OFFICIAL securely.

- This usually is applicable where users need to submit data which can take longer than 1 session.

- User needs to be able to retrieve own data for further updates.

- User needs to be able to update and save the data.

- Once user submits the data, it needs to move to the High Trust for storage and further processing.

- Most of the processing is done on the High Trust.

CDHA features

- Data encrypted using the Browser based User's key.

- Only user holding the private key can decrypt the record on Low Trust.

- Data is encrypted for target users and only the users holding the private key will be able to decrypt the data.

- Each Application user will have its own Key Pairs.

- CDHA works on the Zero Trust principal which means every stage has digital signature verification for repudiation.

- Once submitted, data will travel from the browser session to the High Trust using a combination of users and High Assurance Gateway (HAG) key.