Unikey Overview

Unikey feature description.

Unikey offers

- **...supplier services:**
  With Unikey (in-house central key management), control over key handling is possible on Mercedes-Benz side and can respond quickly to various attacks or leaks. Existing solutions can be used to quickly set up and further develop new technologies. The handling and exchange of crypto material is simplified by the Unikey system.

- **...easy to use (ECU Security Architects):**
  In the future, we are working on establishing a better and simpler request channel via a so-called "landing page" to enable faster support requests. We are also working on a web interface that will allow experienced security architects to receive your requests directly via "self-service".

- **...easy to integrate (Developers):**
  Unikey provides a standardized API interface (oneAPI) to support access from the CI/CD pipeline.

  This allows developers to access required applications directly, quickly and easily via the standardized interface.

- **...easy to adapt:**
  Unikey offers the following crypto operations as a service catalogue, listed in the table below.

  In the Description column you will find a short explanation of the basic functions.

  In general, the following procedure applies:
  - Through the so-called security relevance assessment or risk/threat analysis and the scoping and protection needs assessment by Security Architect and the ECU-supplier, the control unit-specific security requirements for the ECU-project are defined.
  - At the request of the Security Architect, the Unikey UsecaseOwner generates the required key material in Unikey. (The key certificate is generated based on the supplier's ECU-information).
  - The individual keys of the ECU-project are provided to the ECU-supplier by the Security Architect. The provision takes place via a secure channel

    Subsequently, the main functions such as encryption and signature creation can be generated in Unikey via a CI/CD pipeline.

Crypto Operation	Details	Link
Create key	Creates synchronous and asynchronous keys (e.g. RSA, ed25519, AES, ECC, ECDSA) and stores them in crypto-backend of Unikey-System	
Create certificate	Creates certificates e.g. X-509	

Import key	Import an existing key in crypto-backend of Unikey-System	
Verify key	Verifies the authenticity of a key	
Verify certificate	Verifies the authenticity of a certificate	
Encrypt data	Encrypts data (e.g. ECU software) with a symmetric key (AES)	Encrypt API
Decrypt data	Decrypts e.g. asymmetrically encrypted secret (key, password)	
Sign data	Creates a signature from a passed data (e.g. hash of a software) with a corresponding key	Sign API
Send data	Exchange of crypto material (e.g. key, signature, certificate, encrypt data) with HW supplier	