irdeto

Building a Secure Future.™

Datasheet

Flexible Policy-Based Digital Keys For Today Profitable Shared Mobility For Tomorrow

PROFITABILITY

- Supports emerging shared mobility business models, right out of the box
- Reduces hardware cost by leveraging a secure software solution that can directly run on most automotive MCUs.

FLEXIBILITY

- Owners can control when, how and by whom the vehicle is used, via policy-based vehicle access and customization, for multiple users.
- Adapts to real-life situations, such as loss of smartphone and vehicle connectivity

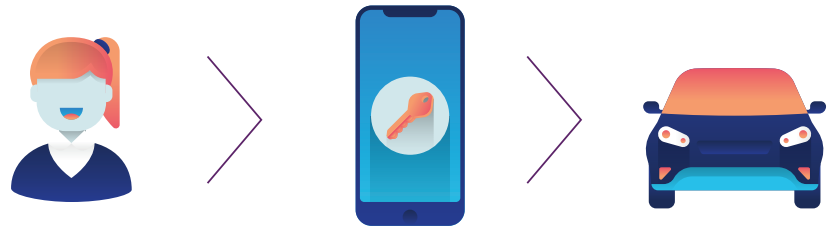
SECURITY

- Provides a proven secure digital key solution that mitigates well-known security threats affecting today's digital key systems, such as: Man-in-the-Middle, Replaay, Amplified Realy and smartphone or access credential theft.

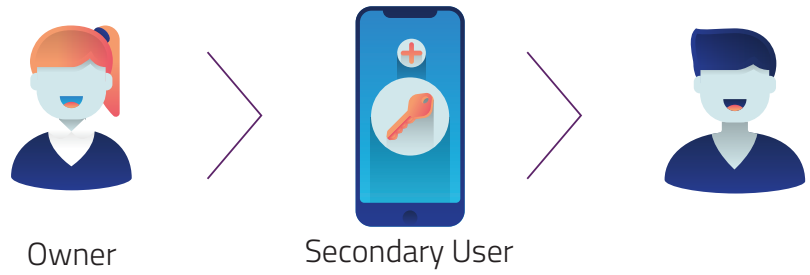
ENABLING SHARED MOBILITY

Keystone helps OEMs enhance the vehicle users' experience by allowing time, feature and geography-based key sharing and revocation directly from a smartphone, while protecting the vehicle owners from malicious use. The flexible and secure key distribution and lifecycle management offered by Keystone is the cornerstone to enabling new connected mobility business models and future-proofing the OEM's business.

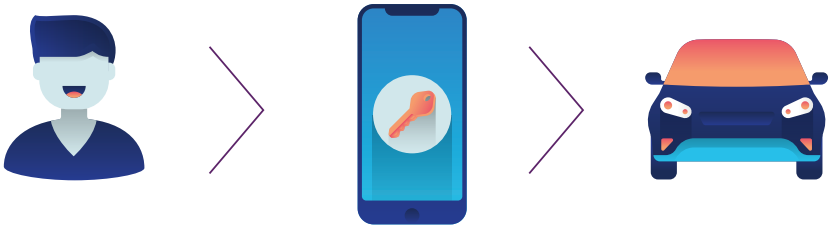
Simple owner pairing process with vehicle



Owner creates secondary digital key and policy



Secondary user has access per policy

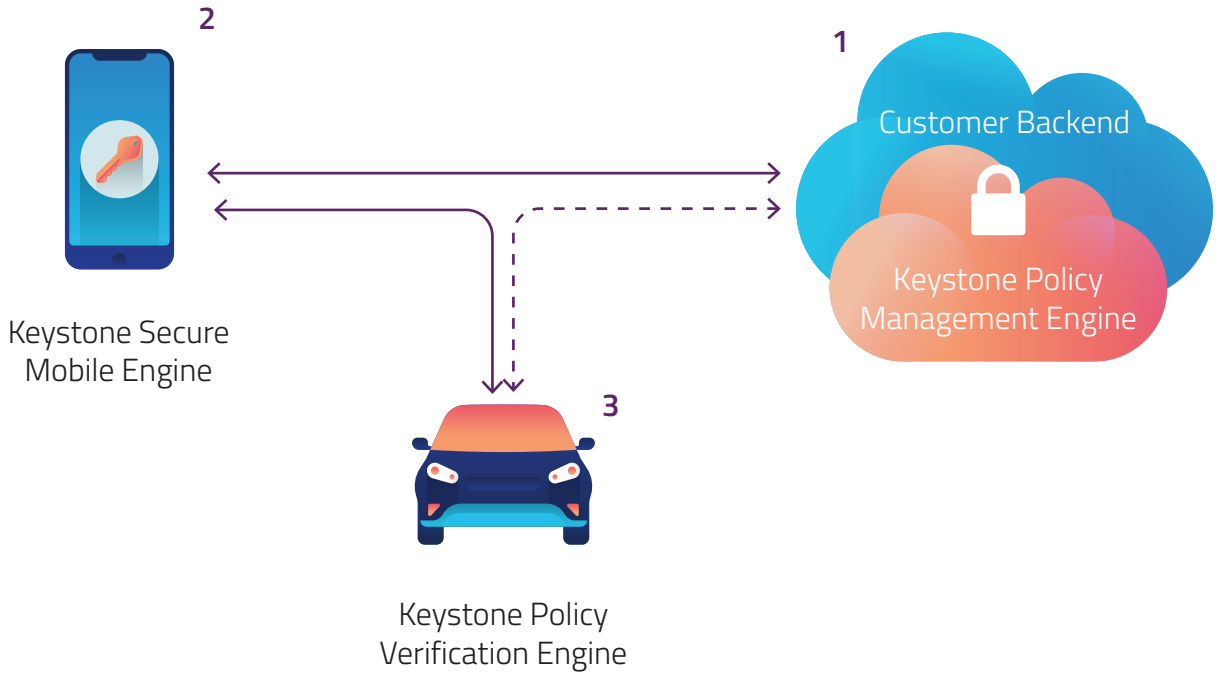


KEYSTONE ECOSYSTEM

1. Keystone Policy Management Engine (Cloud-based backend)
Provides a set of APIs for key life cycle management, policy administration and a notification engine. These can easily be integrated with existing connected vehicle solutions.

2. Keystone Policy Verification Engine (In-vehicle Application/SDK)
Receives and validates commands from the mobile device and acts in accordance with the user's digital key and policy. Integrates easily with major MCU platforms and providers.

3. Keystone Secure Mobile Engine (Mobile Application/SDK)
Uses BLE, NFC or other desired communication technology to issue commands (such as open door, authorize engine start) and pre-condition the vehicle. A mobile SDK handles all management, security and communication, allowing app developers to focus on the user experience.



KEYSTONE FEATURE LIST

- **Login** – allows the user to login into the system securely. During the login process, all required user information, policy, and meta data are syncronised between cloud and mobile securely.
- **Factory Provisioning** – provisioning of the hardware so that it can communicate with the cloud and mobile securely.
- **Owner Registration** – allows user to take responsibility of the vehicle and grant access to create other virtual keys
- **Virtual Key Sharing** – the owner can share keys for a vehicle with multiple users.
- **Revoke Users** – owners can request revocation of the users from list of authorized users. Users can unpair their phones using any other phone in the case of lost/stolen phone.

DEPLOYMENT OPTIONS

Component	Options	
Cloud	Hosted by Irdeto	Hosted by customer/3rd party
Mobile Application	Irdeto's App	Integration with customer's app
Keystone Policy Verification Engine	Integrated by Irdeto	Integrated by customer/3rd party

SYSTEM REQUIREMENT FOR CLOUD INSTALLATION

The Keystone Policy Management Engine has the following database requirements*:

Database: Postgres

Database version: 9.6+

We deploy against a Kubernetes cluster. This deployment has the following minimum requirements*:

- 9 Virtual Machines for the Kubernetes cluster
- 1 Virtual Machine for administering the cluster
- Networked file system for storage (100 Gb)
- User token verification service
- Registration / ownership verification service

***(other deployment options can be investigated on request)**

All Kubernetes nodes should adhere to the following minimum specifications:

CPU: 2 cores

Memory: 4 GB

OS: Linux

Software:
Kubernetes v1.13
Docker v18.09 (API version 1.39)
CFSSL
Helm 2.13.1

The Kubernetes Administration Node should adhere to the following specifications:

CPU: 2 cores

Memory: 4 GB

OS: Linux

Software:
Kubespray v2.9.0
Python 3 and PIP 3
Ansible 2.7.0
SSH Client

Note: These are the minimum requirements in case the cloud is hosted by customer or 3rd party. Other deployment options/requirements can be investigated on request

The Keystone Policy Management Engine expects that a load balancer has been setup, is being managed, and meets the following requirements:

- TLS termination occurs at the load balancer with a valid TLS certificate.
- All connections are made over TLS to the Keystone Policy Management Engine running on port 443.
- The TLS certificate used with Keystone Policy Management Engine are added / accepted by the load balancer.

The Keystone Policy Management Engine expects a database to which all data requiring persistent storage will be written.

- This requires Postgres version 9.6 or higher.
- All connections to the database should be secured with TLS.

SYSTEM REQUIREMENTS FOR MOBILE APPLICATION

Following are the minimum requirements to successfully deploy the Mobile Application:

- Android Studio that supports development on devices running the latest Android Studio version (tested on Android Studio 3.5)
- Android device with Android 8.0 or above
- Xcode that supports development on devices running the latest xcode version
- iOS devices with latest or latest-1 iOS

(The deployment of mobile application can be checked with other versions, if required.)

SYSTEM REQUIREMENTS FOR EMBEDDED COMPONENT

Following chipsets are currently supported:

- NXPS32K
- nRF52840
- RH850x
- TCC803x

Following toolchains are currently supported:

- GCC
- GHS
- IAR

Following CPU architectures are currently supported:

- ARM
- V850

Pre-requisites for platform :

- Secure boot
- Secure storage for cryptographic keys
- HW Crypto operations
- Non-volatile memory (NVM) for Keystone Policy Verification Engine
- ~4KB flash for data storage
- ~400KB flash for code
- BLE 4.x or above

(Note: Support for additional target platforms is also available and can be investigated on request)
Irdeto can also recommend a hardware partner that perfectly fulfils these requirements.