CAMARA

THE TELCO GLOBAL API ALLIANCE

Device Card Binding Mgmt

- China Telecom
- Contacts: chenfr2@chinatelecom.cn

Use Cases

Reason :

To safeguard the security and compliance of IoT devices, measures are often taken to bind the device to a specific card. This mechanism helps prevent the device from being stolen or misused while reducing the risk of data leakage. Once it detects that a card has been separated from a device, the system will automatically disconnect from the network and send a real-time alert to the customer.

Mature Fields

New Potential Valued Fields

public service

Financial

Smart City

Smart Retail

In industrial automation, numerous sensors and controllers connect to the network via SIM cards for real-time monitoring and control of production processes. Device-SIM binding ensures these SIM cards can only be used on authorized sensors or controllers, preventing tampering or unauthorized use and securing production data and process continuity.

Statement of operations

CAMARA
THE TELCO GLOBAL API ALLIANCE

API Integration

The Device Card Binding Mgmt API is registered to the public service application of China Telecom's API gateway.

Customer applies for APPKEY and APPSECRET of the gateway API, then calls the Device Card Binding Mgmt API via HTTP/HTTPS to query and subcribe the relevant risk control information of the IoT SIM card.

Revenue Model

Fees are charged monthly or annually based on the number of cards querying the Device Card Binding Mgmt API.

Current Scale

Currently China Telecom has about 30 million IoT cards subscribing to machine-card binding services.

The API definition proposal(bind)

CAMARA
THE TELCO GLOBAL API ALLIANCE

API Name	Device Card Binding Mgmt Bind API
Description	This API allows enterprise customers to bind imei to the card, when the imei is not match with the bind information, operator will block the network, when the imei is match, resume the network.
Input Parameters	• device(Device): The developer can choose to provide the below specified device identifiers: ipv4Address, ipv6Address, phoneNumber,networkAccessIdentifier.
	• bindInfo(string): Such as bind imei
Return Results	• bind operation status, success or fail

The API definition proposal(unbind)

CAMARA
THE TELCO GLOBAL API ALLIANCE

API Name	Device Card Binding Mgmt Unbind API
Description	This API allows enterprise customers to unbind imei to the card.
Input Parameters	• device(Device)： The developer can choose to provide the below specified device identifiers: ipv4Address, ipv6Address, phoneNumber,networkAccessIdentifier.
Return Results	• unbind operation status, success or fail

The API definition proposal(query)

CAMARA
THE TELCO GLOBAL API ALLIANCE

API Name	Device Card Binding Query API
Description	This API allows enterprise customers to query risk control information related to IoT SIM cards, such as machine-card binding. With this information, enterprises can assess the security and reliability of IoT cards, helping to assess security, detect, and prevent possible fraud.
Input Parameters	• device(Device)： The developer can choose to provide the below specified device identifiers: ipv4Address, ipv6Address, phoneNumber,networkAccessIdentifier.
Return Results	• code(string): Returns the result identifier • message(string): return result description • result (object): Card arealimit or imeibind status

The API definition proposal(subscribe)

CAMARA
THE TELCO GLOBAL API ALLIANCE

API Name	Device Card Binding Subscipition API
Description	This API allows enterprise customers to subscribe to risk control information related to IoT SIM cards. When the device bound to the IoT card changes, the customer can be notified in a timely manner through the callback address registered by the customer, making it convenient for the customer to identify endpoint risks in a timely manner.
Input Parameters	• device(Device)：The developer can choose to provide the below specified device identifiers: ipv4Address, ipv6Address, phoneNumber,networkAccessIdentifier.
	• sink(string)：The address to which events shall be delivered using the selected protocol.
	• sinkCredential(SinkCredential)：A sink credential provides authentication or authorization information necessary to enable delivery of events to a target.
Return Results	• code(string): Returns the result identifier • message(string): return result description • id(string): SubscriptionId