Mastercard KAR Tillegg
Web Service for Business

Technical specifications
Version 3-0

1 Contents

2

1. Introduction

1.1. Document Purpose

The purpose of this document is to describe the technical specification for the REST-based web services for accessing KAR via Mastercard/Nets by using a client certificate.

It is Mastercard who owns the service, but it is run on the Nets infrastructure.

The documentation is intended for developers and technical people.

1.2. Revisions

Version / Date	Description
1-0 – 01.12.2015	First official version.
2-0-17.12.2021	Changed from Nets to Mastercard
3-0 – 17.01.2021	Updated with security certificate description and ruke change regarding who can ask which question

2. KAR Tillegg service

The service enables companies to verify if an account number is valid and if a given person/company owns a given account. The advantage is to ensure correct payments and save time and money used on mistakes.

There are two questions available

- Is the account valid? You send in the account number and get a confirmation ok or a rejection (no)
- Does this person/company own this account? You send in the account number and personal ID or organisational number and get a confirmation ok or a rejection (no)

The company must have an agreement with their bank.

All companies can ask about valid account and ownership for companies (org. nr.). Ownership for a person can be asked by all companies except from a sole proprietorship .

3. REST interface

3.1. Principle

The KAR rest services detailed specifications are described by BSK in the document:

BSK Grensesnitt for Felles Konto- og Adreseregister (KAR) v1-1, date 20.05.2015

This document merely describe Mastercard modification to the BSK interface description.

Where BSK document specify:

https://host:port/kar-ws/api/v1/accounts/{account}/karVerifyAccountPayment

Nets uses:

https://ajour.nets.no/kar-direct/accounts/{account}/karVerifyAccountPayment

In other words, Mastercard do not make any modifications to the semantics of the Web services. The Mastercard modification consist of specifying the *domain name* and the *contextpath* to be used. The domain name being ajour.nets.no and the contextpath being kar-direct.

3.2. REST Web service specification

Refer to chapter 4 of the BSK documentation for the 2 functions implemented by Mastercard:

- karVerifyAccountPayment See chapter 4.3 in the BSK document
- karVerifyAccountOwner See chapter 4.4 in the BSK document

Request, response, error codes and examples are described in the indicated chapters.

4. HTTPS and certificates

Our REST services are protected by 2-way SSL. Mastercard/Nets is at the server side. The consumer is at the client side. Client needs to provide a certificate that is used to authenticate the consumer at the server side.

In order to communicate with the server, the consumer (client) needs the following:

- A client certificate

Mastercard will provide you with a client certificate; one for test- and one for production environments.

The client certificate needs to be created and signed by Mastercard. Your business contact in Mastercard will provide support for getting a client certificate.

Mastercard requires an *email address* to receive the certificate and a *mobile number* to receive the password which is used to install the certificate.

4.1. Renewal of the certificates

The certificate will be valid for 2 years. 90 days before the certificate becomes invalid, you will be notified in an email based on the email-adress that was given Mastercard in the agreement with the bank. Then you need to contact Customer Service at Mastercard and ask for a new certificate.