Eurida Connect Certificate Order Form

This form establishes identification of an End User applying for a Eurida Connect Certificate. This form shall be filled in electronically and the signature shall be signed with blue ink. Please return this form to Mastercard Payments Services eSecurity according to instructions in the Eurida Connect User Guide

Certificate Information	
End User Certificate Environment *	<test or production>
Certificate Request *	PKCS#10
End User Data Values	
End User Name *	<certificate owner name (organisation or person)>
End User Contact Info *	<name, email and phone number of the contact person>
Certificate Requestor *	<name, email and phone number of the person in Mastercard Payments Services representing the End User>
Mastercard Payments Services Data Values (only valid for Mastercard Payments Services services)	
Mastercard Payments Services Business Owner *	Kristin Ringstad Kristin Ringstad Kristin Ringstad
Mastercard Payments Services Service *	eFaktura
Certificate Content	
Common Name *	<identifies the owner of the certificate>
Serial Number	<number e.g. organisation number, employee number>
Organisational Unit	<name e.g. business unit, department name>
Organisation Name *	<the formal name of the organisation>
Country *	<name of country>
Key Usage *	<authentication or signing>
Extended Key Usage	<blank, client authentication or server authentication>
Valid *	<defines the validity period in number of years or days. maximum 4

*=mandatory field
<> Please replace the brackets and text with applicable data

Eurida Connect Certificate Order Form

By signing this form you agree to have read and understood the attached End User Requirements.

Date: _____

Signature End User: _____

Date: _____

Signature Mastercard Payments Services Service Business Owner: _____

Date: _____

Signature Mastercard Payments Services eSecurity WebRA Administrator: _____

PKCS#10 Request

--- BEGIN CERTIFICATION REQUEST ---

--- END CERTIFICATION REQUEST ---

*=mandatory field
<> Please replace the brackets and text with applicable data

End User Requirements for Eurida Connect

General

Mastercard Payments Services eSecurity AS (Mastercard Payments Services) operates Eurida Connect Certification Authority (CA) and Registration Authority (RA). Mastercard Payments Services issues certificates (incl. associated private keys) whose function is to support digital signature and authentication. A Eurida Connect certificate will be issued when an End User has accepted the conditions specified in the End User Requirement (this document), hereunder agree to familiarize him/her with the accompanying "Eurida Connect Certificate Policy".

Eurida Connect certificates must not be used in defiance of applicable law, official rule, CP or the corresponding CPS which the certificates have been issued, or in defiance of an agreement with CA or guidelines given by CA. Eurida Connect certificates must not be used for other purposes than explicitly approved by CA.

These conditions govern the relationship between Mastercard Payments Services and the End User with respect to the use and administration of Eurida Connect certificate(s). In the event of inconsistent or conflict between the End User Agreement and the "Eurida Connect Certificate Policy" (CP), the CP shall prevail.

Duties and Obligations of End User

The End User agrees to:

- Only use the Eurida Connect certificates in accordance with the End User Agreement, the current "Eurida Connect Certificate Policy" (CP) or any other applicable agreement with CA.
- Keep his/her private key, activation data, and related password(s)/PIN private, which mean that no other person other than the End User SHALL be given access. "Other person" is regarded as, but not limited to, any member of the End User house hold or family, colleagues, police, public authorities, bank etc.
- Submit accurate, true and correct information during the Certificate application process to the RA and CA.
- Notify Subscriber and/or RA of any errors or changes in Certificate information.
- Protect the key repository (e.g. Smart Card) against malicious software or any other misuse.
- Request revocation of the Certificate immediately if he/she suspects that the key repository, private key, and/or related password(s)/PIN to be lost or compromised, or an unauthorized person has obtained knowledge of the private key or related password/PIN.
- Not use the Certificate once he/she has become aware of or suspects that the Certificate and/or related password have been lost or compromised.

Certificate Request and Approval

Certificate applications, with the required documentation from End User, must be submitted by Mastercard Payments Services' Customer to Mastercard Payments Services Registration Authority. Application approval or rejection is done by the Mastercard Payments Services Registration Authority.

Certificate Expiration

A Eurida Connect certificates expire after four years. The expired Eurida Connect certificate will not be automatically renewed. Mastercard Payments Services therefore recommends that an application for a new certificate is sent to Mastercard Payments Services Registration Authority at least 30 days prior of expiration.

*=mandatory field
<> Please replace the brackets and text with applicable data

Certificate Revocation

Mastercard Payments Services may, at any time and where adequate, without notification in advanced, revoke a Eurida Connect certificate with immediate effect for reasons such as the following:

- by End Users request,
- the private key has been compromised,
- the End User does not comply with the End User Agreement and/or Eurida Connect CP

After revocation, the certificate is invalid. The End User is liable for any damages resulting from use of a revoked certificate. Mastercard Payments Services is not liable for any kind of damages resulting from such use.

Liability of Mastercard Payments Services

CA is not liable to End Users, Subscriber, Relying Party or any other third party for any loss that may occur by acting in reliance on a Eurida Connect Certificate.

CA is not part in any requirement, purchase, consent, delivery or others between the RA, Subscriber and/or End User and third party even if such is signed with a certificate issued by CA under the Eurida Connect CP. CA has no responsibility with regard to the services or goods delivered based on the trust of the certificates.

Issuance of certificates in accordance with this document or any relevant CP does not make CA an agent, trustee or other representative of Relying Parties or any other third party.

Liability of the End User

End User is liable for documented direct loss if:

- End User use the Eurida Connect certificate in defiance of the terms and conditions in the End User agreement
- End User otherwise commits a material breach of End User obligations.

Personal Information

Eurida Connect certificates issued to End Users may contain personal information.

Information included in the certificate is regarded as public information and will be revealed to third party when using the certificate.

Other personal information provided when ordering a Eurida Connect certificate will be handled in accordance with the Norwegian Personal Data Act (“Personopplysningsloven”).

*=mandatory field
<> Please replace the brackets and text with applicable data