Registers of Scotland PKI-DRS

PKI Disclosure Statement

Release	Date	Comment
1.0	08/2007	Initial publication to website.
2.0	07/2021	Updated text from Entrust. Republished to website.
2.1	07/2026	Updated URL. Republished to website.

Important Notice
The purpose of this document is to:

- Summarise the key points of the PKI-DRS Base Certificate Policy document for the benefit of Subscribers and Relying Parties.
- Provide additional detail and further provisions that apply to the PKI-DRS Base Certificate Policy document and which are incorporated in it by reference.

This document (PKI Disclosure Statement) does not by itself constitute the full Certificate Policy under which Certificates issued by the RoS Issuing CA are governed. You must read the Base Certificate Policy document at https://www.ros.gov.uk/services/digital-discharge-service/dds-for-lenders-t-and-c before you apply for or rely on a Certificate issued by the RoS Issuing CA.

The full Certificate Policy, hereafter referred to as the Certificate Policy, under which Certificates are issued is defined by two documents:

- The PKI-DRS PKI Disclosure Statement (this document).
- The PKI-DRS Base Certificate Policy document.

Terms used in this document are defined in the Registers of Scotland PKI-DRS Glossary of Terms located at https://www.ros.gov.uk/services/digital-discharge-service/dds-for-lenders-t-and-c.

1. Policy Authority & Issuing Authority Contact Info:

1. Policy Authority:

The Keeper of the Registers of Scotland is the Policy Authority for the PKI-DRS. Day-to-day responsibility for the Policy Authority role is delegated to the Policy Authority Function Group (PAFG).

Mailing Address:
Policy Authority Function Group
Registers of Scotland
Meadowbank House
153 London Road
Edinburgh
EH8 7AU

email: PAFG@ros.gov.uk

2. Issuing Authority:
RoS Issuing CA

Mailing Address:
RoS Issuing CA
Registers of Scotland
Meadowbank House
153 London Road
Edinburgh
EH8 7AU

email: PAFG@ros.gov.uk

2. Certificate Type, validation procedures and usage:
The Certification Services provided by the RoS Issuing CA implement a closed public key infrastructure in the sense that access and participation is only open to those who both satisfy eligibility criteria and are approved by the RoS Issuing CA. The Participants providing trust services and End-Entities authorised and approved to issue, obtain, use, and/or rely upon Certificates that reference this PDS are clearly defined. Participation is conditional upon agreeing to be bound by the terms of the Certificate Policy.

The Certification Services provided by the RoS Issuing CA support secure operations and interactions with agent organisations and customers and external contractors in the direct pursuit of Registers of Scotland digital registration services, or in the authorised usage of services provided by the RoS Issuing CA. Certificates provided by this service, are supported by the use of strong cryptography and highly robust registration mechanisms to a defined and assured level of trust and security.

Certificates issued under the Certificate Policy may only be used in conjunction with Registers of Scotland digital registration services; no other usages are permitted. Certificates used for creating electronic signatures may not be used for other purposes.

3. Reliance Limits:
The RoS Issuing CA does not set reliance limits for Certificates it issues. Reliance limits may be set by applicable law or by agreement. See Limitation of Liability below.

4. Obligations of Subscribers:
Subscribers must comply with the requirements as defined in the PKI-DRS Subscriber Agreement and PKI-DRS Base Certificate Policy at https://www.ros.gov.uk/services/digital-discharge-service/dds-for-lenders-t-and-c.

It is the responsibility of the Subscriber to:

- Ensure all information submitted in support of a certificate application is true and accurate
- Review the issued Certificate to confirm the accuracy of the information contained within it before first use
- Prevent any loss, disclosure, or unauthorised use of the Private Key
- Keep Private Keys confidential
- Keep confidential, any passwords, pass-phrases, PINs or other personal secrets used in obtaining authenticated access to Certificates and PKI facilities
- Make only true and accurate representations to the Registration Authority and/or Issuing Authority as to the information required to determine eligibility for a Certificate and for information contained within the Certificate

- In accordance with the Certificate Policy, exclusively use the Certificate for legal purposes and restricted to those authorised purposes detailed by the policy
- Immediately notify the Registration Authority of a suspected or known compromise of Certificate security in accordance with the procedures laid down in the Certificate Policy.

WARNING: If a Subscriber's Private Key is compromised, unauthorised persons could decrypt or sign messages with the key and commit the Subscriber to unauthorised obligations.

5. Certificate Status checking Obligations of Relying Parties:
Relying Parties must comply with the requirements as defined in the PKI-DRS Relying Party Agreement at https://www.ros.gov.uk/services/digital-discharge-service/dds-for-lenders-t-and-c.

A Relying Party may justifiably rely upon a Certificate only after:

- Ensuring that reliance on Certificates issued under the Certificate Policy is restricted to appropriate uses (see "Certificate Type, validation procedures and usage", above for a summary of approved usages).
- Ensuring, by accessing any and all relevant Certificate Status Information, that the Certificate remains valid and has not been Revoked.
- Determining that such Certificate provides adequate assurances for its intended use.
- Take any other precautions prescribed in the Certificate Policy.

6. Limited Warranty & Disclaimer/Limitation of Liability:
The Issuing Authority assumes no liability whatsoever in relation to the use of Certificates or associated Public/Private Key pairs issued under the Certificate Policy for any use other than in accordance with the Certificate Policy and any other agreements. Subscribers will immediately indemnify the Issuing Authority from and against any such liability and costs and claims arising therefrom.

The Issuing Authority shall not be liable for any consequential, indirect or incidental damages, nor for any loss of business, loss of profit or loss of management time, whether foreseeable or unforeseeable, arising out of breach of any express or implied warranty, breach of contract, delict, misrepresentation, negligence, strict liability however arising, or in any other way arising from or in relation to the use of or reliance on, any Certificate except only in the case of the Issuing Authority's negligence, wilful misconduct, or where otherwise required by applicable law.

Nothing in the Certificate Policy excludes or restricts liability for death or personal injury resulting from negligence or the negligence of its employees, agents or contractors.

The Issuing Authority excludes all liability of any kind in respect of any transaction into which an End-Entity may enter with any third party.

The Issuing Authority is not liable to End-Entities either in contract, delict (including negligence) or otherwise for the acts or omissions of other providers of telecommunications or Internet services (including domain name registration authorities) or for faults in or failures of their equipment.

Each provision of the Certificate Policy, excluding or limiting liability, operates separately. If any part is held by a court to be unreasonable or inapplicable, the other parts shall continue to apply.

7. Applicable Agreements, Certification Practice Statement, Certificate Policy:
Copies of this document, the PKI-DRS Base Certificate Policy document, PKI-DRS Subscriber Agreement, PKI-DRS Relying Party Agreement, and the PKI-DRS Glossary of Terms may be updated

from time to time and are published by the Issuing Authority at https://www.ros.gov.uk/services/digital-discharge-service/dds-for-lenders-t-and-c.

8. Privacy Policy:
The RoS Issuing CA strongly believes in an individual's rights to privacy and operates this Certification Service according to the Registers of Scotland Privacy Statement which many be found at https://www.ros.gov.uk/privacy.

9. Refund Policy:
The RoS Issuing CA does not provide refunds for issued Certificates.

10. Applicable Law & Dispute Resolution:
Disputes shall be handled in accordance with the Registers of Scotland complaints procedure which may be found at https://www.ros.gov.uk/support/contact-us/making-a-complaint.

The provision of the RoS Issuing CA Certification Services shall be governed by Scottish law and all parties shall submit to the exclusive jurisdiction of the courts of Scotland.

11. CA & Repository Licences Trust Marks & Audit:
Certificates are manufactured under the Certificate Policy of which this document forms part. Entrust (Europe) Limited provides a Certificate Manufacturing service which is both accredited to ISO27001 and has attained tScheme approval.

Audit shall be carried out on a periodic basis required to maintain security and trust accreditations. The Auditors that have been approved under this policy are:

- Audit resources of contracted Participants providing trust services.
- An auditor or assessor organisation that is approved by Registers of Scotland.

12. Identification of this Certificate Policy:
There is no Object Identifier (OID) for this policy.

13. Approved Registration Authorities
The following Registration Authorities have been approved by the Issuing Authority to register Subscribers under the Certificate Policy:

- Registers of Scotland
- Entrust (Europe) Limited

14. Approved Repositories
The following Repositories have been approved by the Issuing Authority under the Certificate Policy:

- Registers of Scotland
- Entrust (Europe) Limited

15. Eligible Subscribers
The following types of Subscribers are eligible to be issued with Certificates under the Certificate Policy:

- Registers of Scotland staff and other End-Entities under the management of Registers of Scotland.
- End-Entities intending to digitally sign digital discharges through the digital discharge service, if first authorised and approved by Registers of Scotland.

The PKI-DRS Subscriber Agreement can be found https://www.ros.gov.uk/services/digital-discharge-service/dds-for-lenders-t-and-c.

16. Eligible Relying Parties

The following types of Relying Parties are eligible to rely on Certificates issued under the Certificate Policy:

- Registers of Scotland

The PKI-DRS Relying Party Agreement can be found at https://www.ros.gov.uk/services/digital-discharge-service/dds-for-lenders-t-and-c.

17. Certificate Status Information

Certificate Status information is made available via Certificate Revocation Lists (CRLs) and shall be published, at a minimum, every 24 hours.