

Registers of Scotland PKI-DRS

Frequently Asked Questions (FAQ)

Release	Date	Comment
1.0	07/2021	Initial publication to website.
1.1	07/2026	URL updated

What is PKI-DRS?

RoS operates a public key infrastructure for its digital registration services (PKI-DRS) which allows subscribers to digitally sign digital discharges as part of the Digital Discharge Service (DDS).

Who can subscribe to PKI-DRS?

The only eligible subscribers are employees in lending institutions or attorneys operating on behalf of lending institutions who intend to digitally sign digital discharges through DDS.

How are subscribers' identities authenticated?

A team leader within an institution using PKI-DRS nominates prospective subscribers and a separate individual with access to that institution's HR system vouches for the identities of those prospective subscribers. The only information shared with RoS is the name and work e-mail address of prospective subscribers. RoS thereafter confirms with the prospective subscribers that they are happy to proceed with PKI-DRS enrolment.

What is the enrolment procedure?

Following subscribers' acceptance of the PKI-DRS Subscriber Agreement from their work e-mail address, RoS promptly downloads a digital certificate onto a smartcard secured by a temporary PIN, and despatches it to them. If requested, the digital certificate download process can be viewed remotely by the subscriber. Once the subscriber receives the smartcard, they arrange an activation call with RoS, at which point the temporary PIN is revealed to the subscriber who immediately changes it to ensure nobody else can access the smartcard thereafter.

What security responsibilities are placed on subscribers?

Subscribers must keep their PIN secret and keep their smartcard safe and secure. If the smartcard or PIN are compromised, or if signing capability is no longer required, the subscriber must inform RoS immediately, preferably from their work e-mail address, so that the digital certificate can be permanently disabled by being added to a certificate revocation list. RoS will also consider all requests for revocation from sources other than the subscriber. Revocation will be performed promptly by RoS or our PKI supplier, Entrust (Europe) Limited after detection of a compromise or any other event giving cause for revocation. Notification may be issued to the subscriber following digital certificate revocation. If the PIN is entered incorrectly three times in a row the smartcard will be locked, and the enrolment process must be carried out again.

Can I access PKI-DRS any other way?

No, RoS provides the sole means for PKI-DRS subscribers to apply electronic signatures to electronic documents within DDS.

Can I use my smartcard and digital certificate for other purposes?

The digital certificates and smartcards issued by RoS cannot be used for any other purpose.

Where can I use my smartcard and digital certificate?

PKI-DRS digital certificates and smartcards are intended for use in home and office working environments within the UK only.

What are the digital certificate and smartcard technical specifications?

RoS downloads X509 compliant digital certificates which use the SHA-256 cryptographic hashing algorithm and incorporate 2048 bit public/private key pairs onto FIPS 140-2 level 3 smartcards. The digital certificate and smartcard support no other functions than the performance of digital signatures on digital discharges within DDS.

Are signing events logged?

Signing event logging is not part of the PKI-DRS service, but digitally signed digital discharges become part of the Land Register application record once registered and bear evidence of the signing event.

How much does the service cost?

RoS provides the PKI-DRS service free of charge.

Where can I access PKI-DRS documentation?

All documentation relating to PKI-DRS is available at <https://www.ros.gov.uk/services/digital-discharge-service/dds-for-lenders-t-and-c>