Key Recovery Server for Security Manager

Maintain continuity of access — without sacrificing security

The Entrust Key Recovery Server (KRS) for Entrust Security Manager™ provides a highly secure secondary means of accessing private keys used to encrypt information. KRS offers an empowering solution to the increasingly common challenge of enabling and/or maintaining continuity of access to encrypted information when the original private key cannot be accessed by the user.

Securely recover private keys

Our KRS architecture delivers the critical security required to maintain trust across the PKI.

COMMON SCENARIOS FOR RECOVERING INACCESSIBLE PRIVATE KEYS

- Forensic recovery cases
- User death
- Employee departure
- Real-time monitoring
- User self-recovery

Established compliance

Compliant with a variety of established key recovery policies and models, including those adopted by the Federal Common Policy and the U.S. Department of Defense PKI.

Secure control

Enforce separation of roles, easily limit key recovery decisions to specific groups, and implement multi-party oversight/authorization.

- Limit key recovery by policy object identifier (OID)
- Add comments to transactions that become part of the signed transaction
- Configure custom email notifications

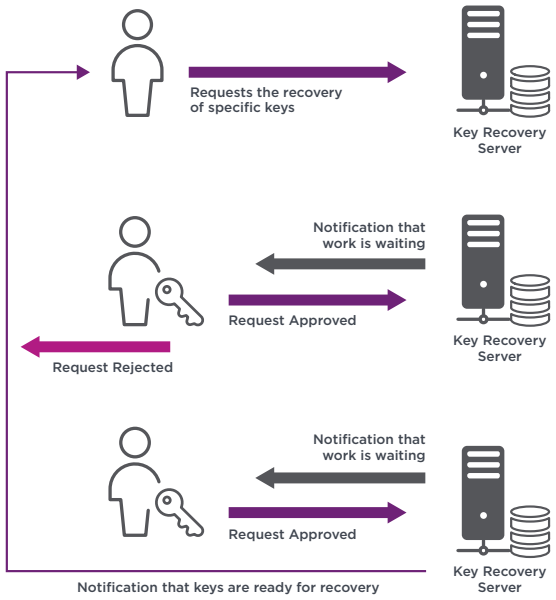
Flexible recovery

Securely deliver keys to the requestor in PKCS#12 format or onto hardware devices.

Key Recovery Server for Security Manager

Third-Party key recovery workflow

When a third-party key recovery scenario arises, the specially designed KRS technology presents a streamlined workflow for executing two-party review and authorization of the key recovery request. See the below example:



1) A key requestor makes a request to recover one or more of a user's keys.
2) The request is queued for Key Request Agent 1 (KRA1). An email notification is generated notifying all KRA1 group members — as well as any other pertinent individuals, such as security officers or Legal — that a key recovery process has commenced.
3) KRA1 retrieves and reviews the request to determine appropriateness and adherence to policy/agency guidelines. KRA1 can then approve or reject the request, or allow it to expire.
4) If approved by KRA1, an email notification is generated to alert Key Request Agent 2 (KRA2). KRA2 reviews the request to determine appropriateness and adherence to policy/agency guidelines. KRA2 can then approve or reject the request, or allow it to expire.
5) If approved by KRA1 and KRA2, the requestor is notified that the request has been approved and the keys are ready for recovery. The requestor may recover the keys to an approved storage format.

Automated key recovery and user self-recovery

Automated key recovery

KRS provides a RESTful interface that allows authorized systems to make key recovery requests in order to perform email or communications monitoring, enforce compliance, or decrypt data that is to be archived. Keys may be retrieved by user, date range, or maximum number of keys. Applications may be limited by policy to specific groups, allowing organizations to limit key retrieval to their specific users.

User self-recovery

KRS now provides a simple process for end-users to retrieve their own encryption keys in order to decrypt data that was encrypted with an older key – or to load the key onto a device, such as a mobile phone – so the user can read encrypted email. An end-user authenticates to KRS using their current credentials, and is presented with a selection of their key history that is available for recovery. Recovered keys are delivered as PKCS#12 encrypted files, or may be loaded onto a hardware token. User self-recovery may be enabled or disabled by the organization.

Learn more at
entrust.com

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379

U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223
info@entrust.com entrust.com/contact