Problem Statement:

Technology developers and administrators need an easy, consolidated, and governable way to monitor and manage secret, key, and certificate expirations, renewals, and rotations.

Details:

Creating software and technology systems in the modern world require that developers and administrators provide applications access to other systems in order to access data managed by another company, piece of software, database or any other system that may be managed separately from the system being developed. Additionally modern software standards encourage and require the need for secure communications and secure access.

These needs require developers and administrators to utilize secrets, keys, and certificates (further referenced as SKCs) to control and secure the access, authorization, and transmission of data. In many cases, these secrets, keys, and certificates are managed in various different places, and are typically generated and setup by many different members among various teams who are all working in effort of the same project or goal. Also, these SKCs are usually configured to expire after some period of time, per security principles and practices. T

Technology teams need a system that can easily allow all users to track when new SKCs are created, when existing SKCs expire, and where the SKCs are all implemented at. This system would alert and notify of upcoming expirations, and aide in keeping documented usage of these SKCs so vital tribal knowledge is not lost when a key individual leaves the team. This would help to smooth and facilitate rotation of SKCs so teams can be confident during deployment windows they can rotate SKCs effectively without the worry that an SKC was implemented in a place that will only be known once a critical bug has been reported by an end user.