



Computing

# Project Close-Out Report

## “KCA End of Life”

---

Version 1.0

2016-10-31

DocDB # 5846

PREPARED BY:

Matt Crawford

CONCURRENCES:

\_\_\_\_\_  
Jon Bakken  
Project Sponsor

\_\_\_\_\_  
Date

\_\_\_\_\_  
Rob Roser  
CIO

\_\_\_\_\_  
Date

<Official copy is maintained electronically – printed copy may be obsolete>

## Project Close-out Report Revision Log

Revision	Description	Effective Date
1.0	Submitted for approval	2016-10-31

# Table of Contents

1.	PROJECT ABSTRACT .....	1
2.	PROJECT DOCUMENTATION .....	1
3.	SUPPORTING DOCUMENTATION .....	1
4.	REASON FOR CLOSING THE PROJECT.....	1
5.	PROJECT DELIVERABLES.....	1
6.	PROJECT SCHEDULE .....	1
7.	PROJECT TEAM .....	1
8.	BUDGET AND FINANCIAL INFORMATION .....	1
9.	OUTSTANDING RISKS.....	2
10.	OPERATIONS AND SUPPORT .....	2
11.	NEXT STEPS .....	2
12.	LESSONS LEARNED.....	2

## 1. Project Abstract

This project began with the intention of upgrading the hash algorithm used by the KCA (Kerberized Certificate Authority) from SHA-1 to one of the SHA-2 family of hashes. It was repurposed to instead oversee the orderly end of support for the KCA and the conversion of dependent services and their users to other supported methods of authentication.

## 2. Project Documentation

Documentation of the KCA shutdown and the alternative steps users should take has been inserted into previously existing Service Now Knowledge Base articles that mentioned the KCA. The Authentication service description has been updated to say the KCA service is deprecated.

## 3. Supporting Documentation

Project documentation is in CD DocDB document #5846.

## 4. Reason for Closing the Project

The conversion of services to other authentication methods was completed on September 29, 2016. As best we can determine, all affected users have been migrated to other authentications systems: either SERVICES or CILogon.

## 5. Project Deliverables

The project delivered announcements to the user community about the termination of the KCA services and pointed users to alternate authentication sources. A series of Change Tasks was generated and assigned to administrators of web sites known by scanning to be accepting KCA certificates for authentication. These Change Tasks pointed out the alternate authentication schemes and urged the administrators to make the necessary changes to shift from using KCA certificates to an alternate. All the Change Tasks were successfully completed—or cancelled in the case of some web sites that were shut down instead.

## 6. Project Schedule

The project began roughly in November of 2015 with a survey of servers. Our self-set deadline for ending KCA support was 30 September, 2016, and we met that. The final shutdown of the KCA will be made at some convenient time in the next few months.

## 7. Project Team

The team consisted of technical lead Frank Nagy and project manager Matt Crawford, with assistance from Al Lillianstrom and Olga Terlyga.

## 8. Budget and Financial Information

There was no budget for this project. Effort was charged to **53.02.11.03.03 SERVERS-SERVICES-OP** through FTL activity **AUTHENTICATION AND DIRECTORY / Project / Service Improvement / KCA Upgrade to SHA-2**. There were no M&S expenditures.

<b>Salary, Wages, and Fringe (SWF)</b>	<b>Reported (FTE•yrs)</b>	<b>Adjusted (FTE•yrs)</b>
Fiscal Year 2016	0.165	0.208
Fiscal Year 2017	0.008	0.010
<b>Total</b>	<b>0.172</b>	<b>0.218</b>

## 9. Outstanding Risks

The very small risk exists that a practical break of SHA-1 could be found and exploited while some Fermilab servers still have the KCA root certificate (or other outdated roots) in their trusted certificate caches.

It is possible that there are users who have been away from the lab for some time and not obtained their CILogon credentials yet, and who might be caught by surprise despite all our communication efforts. We expect few if any such cases and must deal with them as they appear.

## 10. Operations and Support

The KCA is now unsupported. If it fails, it will not be fixed. Operation will cease completely some time between now and the end of January, 2017.

The replacement authentication methods are the SERVICES domain and the CILogon CA, which are not changed by this project.

## 11. Next Steps

The Computer Security Team will survey TLS-speaking servers and probe for acceptance of the KCA or other outdated CAs.

## 12. Lessons Learned

See the "*KCA end of life – Lessons Learned*" document for Lessons Learned.