# Contribution to FIPS 201-3 DRAFT

Proposed new clause 5.5.3

*Gerald "Gerry" Smith*

Generic Smart Cards LLC

**JAN 2021**

## Purpose

This document details a proposed Physical Access Control System (PACS) credential cancelation list under Section 5 PIV Key Management Requirements of FIPS 201-3 (currently in DRAFT form).

Generic Smart Cards LLC proposes to add a new clause 5.5.3, just beyond the CRL (5.5.1) and OCSP (5.5.2) clauses, defining this additional conveyance of trust limited in scope to PACS relying parties.

## Concept

The concept is simple. The issuer would maintain a list, harmonized to the latest CRL(s) available. ANY of (up to four) certificates associated with a given card Universally Unique Identifier (UUID) that have been revoked shall trigger adding of said given UUID to the list. Other conditions, not related to certificate revocation, may trigger adding a given card UUID to the list.

The list itself is envisioned to be a comma separated value (csv) format with two tuples per entry; the card UUID and the date the card UUID was added to list. The reason why a card Universally Unique Identifier (UUID) was added to the list shall not be stated. (Reasons may include the credential was reported lost or stolen, the card holder has been determined in a court of law to have committed a disqualifying offense, or a production error was detected after the card was provisioned).

The list would be posted by the issuer on a regular basis (perhaps harmonized with CRL refreshes or refreshed at a given time interval such as daily). One additional file shall be produced for each new list to provide list verification to relying parties:

a) A PKCS#7 Detached Signature of the list with a dedicated embedded Content Signing X.509 v3 certificate. The public key required to verify the digital signature SHALL be issued under the *id-fpki-common-piv-contentSigning* policy of [COMMON]. Use of the EC-256 algorithm or EC-384 algorithm is encouraged over the aging RSA-2048 algorithm.

Verification might encompass either:

1) Simple verification of the embedded message digest to an externally computed message digest.
2) Signature validation (inclusive of chain of trust validation).

The GSC LLC proposed name for this additional, PAC specific, list is:

## Canceled UUID Liability List (CULL).

The proposed name is inspired from the English definition (from Merriam-Webster):

### Definition of *cull*

*transitive verb*

**1:** to select from a group.

**2:** to reduce or control the size of (something, such as a herd) by removal.

See: Cull | Definition of Cull by Merriam-Webster (merriam-webster.com)

## Rationale

Unlike logical access, PACS solutions generally leverage a credential identifier from which access privileges and other services are then linked.

Having a lightweight revocation solution for PACS that conveys issuer trust status, searchable by credential identifier, would provide many benefits including:

1. Aggregation of all end-entity certificates revocation status carried by the credential to be determined from a single list.
2. Separating credential trust for PACS from trust for logical access. (Example is revoking site access but still permit remote logins).
3. Off-line use lowering the operational costs for maintaining revocation status.
4. Acts as a countermeasure to a specific denial-of-service attack (by interfering with revocation servers).
5. Permits non-PKI aware PACS solutions for physical locations not well served by an “always connected” security framework.

# Proposed Contribution Language

### 5.5.3 Physical Access Control System (PACS) Canceled Credential List

A Canceled card UUID Liability List (CULL) may be implemented per [TBD] enabling relying parties to separate credential use policies related to PACS credential revocation from logical access certificate(s) revocation. For example, a relying party might use the CULL to deny building access but, remote login would rely upon the CRL or OCSP status responders.

# Contact Information

Name: Gerald “Gerry” Smith

Email: Gerry.smith@comcast.net

Cell: +1 804 503 0679