[MS-PAC]: Privilege Attribute Certificate Data Structure

To view a PDF file of the errata for the previous versions of this document, see the following ERRATA Archives:

November 23, 2020 - Download

April 29, 2022 - Download

Errata below are for Protocol Document Version V23.0 – 2022/04/29.

Errata Published*	Description
2022/12/12	The following sections were changed. Please see the diff document for the details. In section 2.4 PAC_INFO_BUFFER: Added new required ulType 0x00000013 for Extended KDC (privilege server) checksum buffer. Changed from: *(table below)* Changed to: *(table below)* In section 2.8.1 Server Signature: Added that the server signature MUST be generated AFTER the extended KDC signature. Changed from: … The resulting hash value is then placed in the Signature field of the server's PAC_SIGNATURE_DATA structure.

Changed from:

Value	Meaning
. . .	
0x00000012	PAC Requestor indicates that the buffer contains the SID of principal that requested the PAC (section 2.15). PAC structures MUST contain one buffer of this type.<9>

Changed to:

Value	Meaning
. . .	
0x00000012	PAC Requestor indicates that the buffer contains the SID of principal that requested the PAC (section 2.15). PAC structures MUST contain one buffer of this type.<9>
0x00000013	Extended KDC (privilege server) checksum (section 2.8). PAC structures MUST contain one buffer of this type. Additional KDC checksum buffers MUST be ignored.

Errata Published*	Description
	Changed to:
	… The resulting hash value is then placed in the Signature field of the server's PAC_SIGNATURE_DATA structure.
	The server signature MUST be generated AFTER the extended KDC signature (section 2.3.4).
	Section 2.8.3 Ticket Signature: Added the extended KDC signature in the recompute list.
	Changed from:
	… the KDC SHOULD verify the integrity of the existing ticket signature and then recompute the ticket signature, server signature, and KDC signature in the PAC.
	Changed to:
	… the KDC SHOULD verify the integrity of the existing ticket signature and then recompute the ticket signature, server signature, KDC signature, and extended KDC signature in the PAC.
	Section 2.8.4 Extended KDC Signature: Added new section.
	Describes its usage and contents. It is used to detect tampering of PACs by parties other than the KDC. Describes where to use it in tickets for various accounts. Contains the ulType 0x00000013 same as described in section 2.4 PAC_INFO_BUFFER. Contains the SignatureType and its key. It is comprised of keyed hash of the entire PAC message with all other Signature fields of all other PAC_SIGNATURE_DATA structures set to zero. It is placed in the Signature field of the extended KDC's PAC_SIGNATURE_DATA structure (section 2.8).