This **DRAFT** (NIST Draft SP 800-78-4 [May 2013]) document has been approved as **FINAL**, and has been superseded by the following publication:

Publication Number:	**Special Publication 800-78-4 (FINAL)**
Title:	**Cryptographic Algorithms and Key Sizes for Personal Identity Verification**
Publication Date:	**May 2015**

- Final Publication (2 URLs – (1) NIST Library –or- (2) DOI:
  NIST Library:
  http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-78-4.pdf
  DOI:
  http://dx.doi.org/10.6028/NIST.SP.800-78-4
- Related Information on CSRC:
  http://csrc.nist.gov/publications/PubsSPs.html#800-78
- Information on other NIST Computer Security Division publications and programs can be found at: http://csrc.nist.gov/

The following information was posted to CSRC announcing release of this document:

June 1, 2015:

NIST announces the release of **Special Publication 800-78-4**, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*. The document has been updated to align with updates in SP 800-73-4. The document reflects the disposition of comments that were received on the first and second draft of SP 800-78-4, which was published in May, 2013 and May 2014, respectively. In particular, the following changes were introduced in SP 800-78-4:

- Removal of information about algorithms and key sizes that can no longer be used because their "Time Period for Use" is in the past;
- Addition of algorithm and key size requirements for the optional PIV Secure Messaging key.
- Addition of requirements for Cryptographic Algorithm Validation Program (CAVP) validation testing.
- Clarified that RSA public keys may only have a public exponent of 65 537. (Client applications are still encouraged to be able to process RSA public keys that have any public exponent that is an odd positive integer greater than or equal to 65 537 and less than 2^{256}.)

The complete set of comments and dispositions is provided below.

- Comments Received & Disposition from May 2013 draft to Revised Draft SP 800-78-4
- Comments Received & Disposition from May 2014 draft to Revised Draft SP 800-78-4