Submitted by: ____

Date: ______________

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)
1	Priva Technologies	David West dwest@priva-tech.com	D1 E	Sec 3 page 10	Section 3 states Smart Card as the only form factor for the PIV. There are other form factors in the marketplace i.e. USB tokens, Compact Flash adapters for moble devices and others that when used will provide the same or better level of authentication and security depending on the environment and hardware client device. Flexibility should be included to cover near-term and future requirements when a smart card as proposed may not be a viable physical or system level option. As an industry we must continue our efforts in creativity and inovation. There are also other levels of physical and logical security that can not be addressed in a smart-card form-factor. We do not believe the PIV should be exclusive to any one device or physical representation-- we believe that FIPS 201 should dictate logical messaging structures to help aid in interroperability for various forms of a PIV's that may be required over time.

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editoral, T = technical

Comment template for draft FIPS 201 and SP 800-73

Submitted by: ______________________________

Date: ____________

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)
2	Priva Technologies	David West dwest@priva-tech.com	D1 E	Sec 3 page 10	Section 3 states that this standard is to promote uniformity and interoperability amongst various PIV system components….. There will always be uniformity and interoperability when the standard doesn't allow for multiple basic system components. This is because FIPS 201/SP 800-73 does not allow for a variety of basic baseline standards such as credentials other then an X509 certificate, authentications environments other then PKI and form factor (smart cards). Standards and efforts have been in process to address interoperability without the severe limitation of a specific product. Innovation in security and authentication is mandatory, and should thus be encouraged.
3	Priva Technologies	David West dwest@priva-tech.com	D2 E	Sec 1.1 page 9	How will this new standard interoperate with all of the older standards that now provide guidance today? This standard as it stands today, will over a short period of time, obsolete the Federal Bridge CA, PKI interoperability standard, Smart Card Interoperability Standard and Identity Assurance Interoperability Standard.

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editoral, T = technical

Comment template for draft FIPS 201 and SP 800-73

Submitted by: ______________________________

Date: ____________

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)
4	Priva Technologies	David West dwest@priva-tech.com	D2 E	abstract page 4	SP 800-73 is a radical upgrade to smart card standards, the card manufactures and integrators will have to spend significant amounts of resources to provide this intergraded circuit card environment. This card already has a carve out for certain organizations whereby the requirements are not compatible for certain reasons. Should a file-based system card or similar implimentation prove restricted and flawed over time, there are no existing mechanisms to account for such event without revisiting this specification. Logic Level architecture should be seperate from the actual implimentation in hardware. Variable security levels and models will not all fit in the current specification which is so specific to one PIV. New innovations and better security mechanisms will be stiffled if this is the only specification utilized for PIV compliance.

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editoral, T = technical

Comment template for draft FIPS 201 and SP 800-73

Submitted by: ____

Date: _______________

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editoral, T = technical

Proposed change
the PIV should be based on interoperability of a messaging standard, not the combination of specific physical and logical standard combined as one. Language should extend the PIV to allow for various form factors that can communicate using standards being proferred in the specification. hardware Interfaces should not be specific to the Smart Card inteface, as others may become as important for certain applications (like mobile authentication devices). The standard should for the PIV should include, but not be limited to a smart-card form-factor, but may take on other forms and interfaces with standards complient features. Newer technologies which exist today meet most of the functional requirements but combine standards or technologies to create stronger protection and trust models. Language should address these new innovations as possible PIV alternatives, or at least provide a mechanism to enable additional PIV's to be approved which may fall outside of the scope of existing SP 800-73.

Proposed change
Allow more use of today's industry standard technology for the PIV token and PKI environment. This was achieved in some areas of FIPS 201 (i.e. biometerics ANSI, contactless ANSI, etc) except for the PIV card technical specification (SP 800-73), credentialing (X509 cert) and authentication environment (PKI). Other options for excepting a variety of credentials can be found in FiXs (Federal Cross Credential System) that can except any form of approved credential. Cross credential mechinsms are very important and a section of the specification should address the ability for those system to be acceptable within this standard.
There is no need for these standards if all agencies use only one system and that system does not allow for variety

Proposed change
A proposed change would be utilize SP 800-73 as a base-line, without the physical form factor being locked in. SP 800-73 should be one of specifications utilized, not the only. It is more important to gain an interoperable messaging architecture in this standard such that credentials can be properly issued, managed and validated.

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editoral, T = technical

Proposed change

D = Document,1 = FIPS201, 2 = SP800-73
T=Type of Comment, E = editoral, T = technical