Response to FIPS PUB 201

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section, Annex, etc and Page Nbr	Comment (Include rationale for comment)	Proposed change
1	XTec Inc.	H. Jackson	General	Pg. 1 Introduction	It should be noted that a credential alone does not authenticate. A credential is an artifact that one offers as proof that he or she is what they represent themselves to be. If we accept that proof, then we accept the representation. Generally this proof takes the form of something the person has, or knows, or is, which only this single individual could have. Preferably all three forms are present at the same time. This is generally referred to as three-factor authentication. In order to trust the individual we must have a level of trust in the credential. A low level of trust is gained when we accept the credential at face value. A higher level of trust is gained when we can test the credential in some way that proves it is genuine—a sort of acid test that proves it is really gold and not fool's gold.	
2	XTec Inc.	K.Kozlowski	General		HSPD-12 calls out that the "Standard will include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application." The PIV should state the levels of security.	Include the following levels of security Level 0 – Card is a flash pass Level 1 – Card with data (PACS Low Assurance) Level 2 – Card with signed data (PACS Medium) Level 3 – Card and Data Authentication (PACS High) Level 4 – Level 3 with PIN or Biometric Level 5 – Level 3 with PIN and Biometric
3	XTec Inc.	K. Kozlowski	General		Each agency is at a different level of implementation and has unique requirements. Each agency should be able to decide the level of security to be applied to each access point. Each agency should also be able to decide which technology to choose (example, either	Mandate each PIV card contain technologies in the chip to support authentication via symmetric or asymmetric technology. Allow access control to work either contact or

					contact or contactless technology for access control). The Standard should allow for this flexibility, but mandate for each method/technology details to implement in an interoperable way. This would allow the government to leverage the different successful deployments already in existence.	contactless (cards support both, agency decides which type of readers to install)
4	XTec Inc.	H. Jackson	Technical	Pg. 14 Section 3.3.1	Presenting a PIN to the card to unlock or activate it, does not provide any proof for authentication of the cardholder. In this case, you trust the card to verify the PIN, but you have no proof that the cardholder did not seed the card. All this says is that the cardholder knows what is on the card. For true two-factor authentication, the PIN must be tied to something that is outside the control of the cardholder. Similarly, an on-card biometric does not provide two-factor authentication unless the card itself can be authenticated independently of the biometric. As an example of true two-factor authentication, the PIN is used to derive a secret key on the card. The key is placed on the card by an issuing authority. A challenge-response can be used to authenticate the key and, at the same time, validate the PIN, which is known to the cardholder, but cannot be changed without knowing the secret key known only to the issuer.	Change language as follows: "…The use of biometrics provides an additional factor of authentication when it can be validated independently and in addition to validation of the card. "…A PIN pad allows two factor authentication when the PIN can be validated independently and in addition to validation of the card, and outside the control of the cardholder.
5	XTec Inc.	H. Jackson	Technical	Pg. 14 Section 3.3.1	It is absolutely correct that the only way to have a high assurance that the card is authentic is to use a challenge response. As the draft specification states, there are two possible cryptographic methods that can be used: symmetric and asymmetric (public-private key or PKI). Relying solely on PKI cryptography is not sufficient because: (1) having a single method puts all the eggs in one basket, and security issues will be amplified without the ability to change methods; (2) both PKI and symmetric keys have distribution issues (although different) where one or the other may not be agreeable to the issuing agency; (3) PKI is not suitable for card authentication in physical access control systems due to speed and the need to cryptographically authenticate the whole chain of issuance; (4) there are practical	Add language as follows: "…Both public key and symmetric key cryptographic methods are used for card authentication. The key management component is used throughout the PIV lifecycle to insert private keys and to generate on-card private-public key combinations.

					limitations on the number of certificates that can be issued by a single certificate authority; (5) because PKI requires substantially more processing power than symmetric key cryptography, symmetric keys offer the most viable form of authentication for contactless cards.	
6	XTec Inc.	H. Jackson	General	Pg. 15 Section 3.3.3	It should be noted that Section 6 actually refers to the authentication of the *credential* not the cardholder. Authentication of the credential is the first step in validating that the cardholder is who he presents himself to be.	
7	XTec Inc.	H. Jackson	Technical	Pg. 23 Section 4.1.5	Symmetric keys should be used as well as asymmetric. See comments under item number 1 above.	"…these mandatory data elements include the following: • Symmetric keys used for card authentication
8	XTec Inc.	H. Jackson	Editorial	Pg. 23 Section 4.1.5.2	It should be noted that the Cryptographic Information Application described in SP800-73 is optional as specified in that document.	Add language as follows: "…defines an *optional* Cryptographic Information Application…" "Where the CIA is not present, the card can be expected to conform to GSC-IS, which contains a Card Capability Container that can be used in the same fashion as the CIA."
9	XTec Inc.	H. Jackson	General	Pg. 24 Section 4.1.6	Refer to number 2 above for a comment on the use of PINs for two-factor authentication.	
10	XTec Inc.	H. Jackson	Technical	Pg. 25 Section 4.2.1	The FASC-N, defined in the GSC-IAB PACS document, attempts to redefine the SEIWG, which is a long-standing government specification. As such, the FASC-N is problematic for the following reasons: (1) it changes the SEIWG without accreditation from the original specifications group; (2) it is not a well published specification that creates a useable standard; (3) it redefines portions of the SEIWG in such a way that it	Specify use of the SEIWG as the unique cardholder identifier until a better constructed, simpler, and globally accepted identifier can be defined. One possible scheme is to use a 16-byte number similar to the GUID (see

					distorts the original specification yet cannot be distinguished from the original—both are assigned the same tag value; (4) both the FASC-N and the SEIWG use a complicated encoding scheme—at least one government agency has implemented it incorrectly.	following—item 11).
11	XTec Inc.	H. Jackson	Technical	Pg. 25 Section 4.2.1	The FASC-N is defined in the PACS document as to uniquely identify the cardholder, not the credential. The PIV draft misstates this distinction. Using the cardholder unique ID as the card ID is a bad practice, since the card cannot be revoked. To do so, you would have to revoke the person. A better ID to use, also defined in the PACS, is the Global Unique ID (GUID) number. This ID is simply a 16-byte number that uniquely identifies the credential. It is large enough to assign a unique value to every possible credential. It is also large enough to allocate chunks to different organizations (and countries) that can be used to assign unique numbers without fear of conflicts. Number-chunk allocations can easily be governed by a registration body (for example NIST) similar to IP address allocations by IANA and ARIN.	Use the GUID (defined in the PACS) as the element that uniquely identifies the PIV credential. This element should be made mandatory as part of the CHUID container.
12	XTec Inc.	H. Jackson	Technical	Pg. 26 Section 4.2.2	There are multiple techniques for performing elliptical cryptography, none of which have become a government published standard. ECDSA may have been approved in FIPS 186-2 (digital signature); however, only Certicom has this designation, which is a proprietary algorithm. In order to ensure interoperability, only FIPS published cryptographic standards (like AES and DES) should be called out for inclusion in the PIV.	Eliminate all references to ECDSA .
13	XTec Inc.	H. Jackson	Technical	Pg. 27 Section 4.3	Refer to number 3 above for a comment on the use of symmetric keys in addition to PKI.	"…The PIV shall implement the following cryptographic operations and support functions: • DES or AES secret key cryptographic operations
14	XTec Inc.	H. Jackson	Technical	Pg. 27 Section 4.3	Because transmissions are open to interception, cryptographic operations are essential to contactless card operations. Plus, because PKI requires substantially more processing power than symmetric key	Add language as follows: "…It is strongly recommend that agencies using contactless cards

					cryptography, symmetric keys offer the most viable form of authentication for contactless cards.	implement card authentication utilizing symmetric keys.
15	XTec Inc.	H. Jackson	Technical	Pg. 29 Section 4.3	It should be noted that the CHUID as specified in the PACS document, specifies an Authentication Key Map to be used for inter-agency interoperable card authentication. Since both the CHUID and the PACS documents are called out in the PIV draft specification, interoperable card authentication is, in fact, a part of the PIV.	Change language as follows: "…Cross-agency interoperability for card authentication is provided through the CHUID Key Map.
16	XTec Inc.	H. Jackson	Technical	Pg. 59 Annex A	PC/SC is a software specification for operating system compliant drivers (Windows) to interface with smart card readers. The reader itself does not have to meet any specific requirements, only that the driver supplied with the reader will work in the PC/SC framework. In many situations (physical access control systems, for example) this specification is not relevant.	Remove all requirements that the PIV reader meet PC/SC validation requirements.

Response to NIST 800-73

Cmt #	Organization	Point of Contact	Comment Type (G-General, E-Editorial, T-Technical)	Section, Annex, etc and Page Nbr	Comment (Include rationale for comment)	Proposed change
1	XTec Inc.	H. Jackson	Editorial	Pg. 26 Section 5	The NIST 800-73 document is a speciation for the structure and content of PIV integrated circuit card. As such it should not also include the high-level specification of a software interface for applications that may use the card. This client-application programming interface is essentially a specification for middleware that could be used with any card. Real interoperability is achieved at the card edge interface. Any application could talk directly to the card through the card edge without having to implement the API. The actual interoperability and use of the card has no real bearing on the client software. Additionally, there are many instances (physical access control, for example) where this API has no relevance.	Suggest the Client-Application Programming Interface (all of Section 5) be removed in its entirety.
2	XTec Inc.	H. Jackson	Technical	Pg. 51 Section 6	The card commands in specified in Section 6 are not compliant with NIST IR 6887, the previous government-wide smart card interoperability specification. Many current identity card implementations by government agencies were built to the previous standard. To make these two standards interoperable, NIST 800-73 should include a provision that cards conforming to the earlier standard may be used as long as they have the Card Capability Container. Cards conforming to the new standard would not need the CCC.	Add language as follows: "…The following table lists the card commands on the command platform complying with the current specification 800-73. For backward compatibility with previous NIST smart card interoperability standards, a card command set compliant with NIST IR 6887 may also be use if the card contains the Card Capability Container. Either one or the other set of commands may be used, but they may not be intermixed.
3	XTec Inc.	H. Jackson	Editorial	Pg. 85 Section 7.2.1	The SELECT OBJECT command for the general container application does not specify which objects are available for selection.	

4	XTec Inc.	H. Jackson	Editorial	Pg. 86 Section 7.2.2	The GET PROPERTIES response does not specify the format and content of the returned properties.	
4	XTec Inc.	H. Jackson	Editorial	Pg. 87 Section 7.2.3	Does not specify the content and format of the returned data.	
5	XTec Inc.	H. Jackson	Editorial	Pg. 89 Section 7.2.5	Does not specify the content and format of the returned data. Also references two different kinds of data buffers: one for tags and one for data values. This is not consistent with the data element descriptions in Section 4, which describes a BER-TLV format.	
6	XTec Inc.	H. Jackson	Editorial	Pg. 91 Section 7.3.5	This is the wrong description for the GET CHALLENGE command.	
7	XTec Inc.	H. Jackson	Editorial	Pg. 93 Section 7.3.7	Does not specify the content and format of the returned data	