Before we start this I just want to go over a little clarification of this morning and the differences with the huge investment that has been done starting with the DoD side. The difference is between the words, identity, and authentication and access privileges. This card when issued, will give you the piece of identity and authentication. You need to think of the back-end systems because talking with that card would be where the access privileges come from, whether that's from the computer or that's getting in the door or being looked at by a guard. Anyone wants to sort that out on an offsite discussion or further discussion, please contact me, but identity authentication is one piece in the access privileges or something that is garnered by the trust coming from the identity and authentication. I hope that makes some sense to some.

Okay this session is on PIV2. This session is on PIV2 and I will be specifically talking about the special publications that provide some of the technical details for the framework that FIPS 201 presents. 873 is essentially the card application specification for PIV, 76 is biometrics, and 78 is cryptographic issues. I will spend the bulk of the time on 873 partly because I was more involved with that document and with the others and also partly because the 876 is still sort of influx. It has not actually been published officially, so I will just have one slide on that. Next please. Okay diving right in here. 873 is the way I think is that it is the card application specification for the PIV application domain. A really important point here and one that is I really feel I need to emphasize this because of the GSC world, 873 does not present a general purpose interoperable card platform made to support a wide range of applications. It is a fairly new application definition for PIV and to support HSPD12. The GSC interoperability specification which I will mention occasionally in this presentation was meant to be a fairly broad interoperability framework for smart cards in the government, so they are conceptually different things, although of course they have some connections. 873 is broken into three parts, part 1 talks about the things that are common across different phases, I should say different parts of PIV2. This will become a little clear as I go along, but there is a common data model that applies to both a transitional specification in part 2 and the end point specification in part 3, so we have put this in part 1 and part 1 also talks about some migration issues, migration strategy to some extent. There are a number of agencies that have ongoing or perhaps even completed smart deployments and a number of these are based on the GSC interoperability specification and so in designing 873 we had to take that into consideration that we could not necessarily just start from scratch. We had to think a little bit about how these GSC base deployments might be able to migrate forward. So then part 2 in that spirit presents a transition specification for use by agencies that have GSC base deployments already and this is sort of a middle ground if you will between the previous GSC world and the PIV2 endpoint. Then part 3 is the endpoint specification and this specification is as I said earlier is very much focussed on the PIV application requirements. Really what is meant to do is provide this fairly narrowly defined card application definition to support the requirement of FIPS 201. Next please.

I will not go through and read all of these, but I will just say that the data model, which is common to both the transitional and end-point specifications, contains a number of mandatory credential objects and then a number of optional credential objects. Again, the definition of these objects was very much driven by FIPS 201 and the PIV requirements.

So, I already showed you the mandatory elements. You can read these in 873 easily enough. These are the optional elements. The two things that I will mention in the data model that are of particular significance are that we retained the GSC card capability container or CCC, as it is called, through the end-point specification for discovery purposes. That is its actual use in the GSC world also. So, this lets us provide some continuity from GSC to PIV2 endpoint. The one thing that is not used in the card capability container, as we progress forward, is the mapping of card commands that was done in GSCIS.

So, I already talked about this a bit. There are agencies with ongoing deployments based on the Government Smart Card Interoperability Specification. We are providing continuity of the data model and the one very important thing to understand is that agencies can choose to use the transitional specification for migration purposes or not. So, whether you are an agency with a legacy GSC deployment or an agency starting completely from scratch, you have no smart card deployment that you are not mandated to use this transitional specification. It is there for you to use if you want to.

Part 2, the transitional specification, I guess the easiest way to describe it in one sentence or less, is to say that it is a PIV application profile based on the GSC Interoperability Specification and again the GSC based data model for PIV does carry both across part 2 and part 3. The transitional specification does maintain the original GSC Interoperability Specification concept of 2 different card edges or card command interfaces due to the differences between file system cards and virtual machine cards. It was developed by the Government Smart Card Interagency Advisory Board and provided to NIST for inclusion in 873. So, at this point, it is probably appropriate for me to thank the IAB for all the work they have done in that area again, in addition to their very thorough review of the other parts of 873 that help NIST tighten it up considerably; and part 2 is informative. It is not mandatory.

Okay, so moving on to part 3, the differences between what we have done in part 3 and the older GSC Interoperability Specification work are that we now have a single unified card edge interface, card command interface. This interface is completely compliant with the existing international standards, ISO 7816 in particular. It allows us to have a completely technology neutral architecture all the way down to this card edge. In other words, there is no longer any need to worry about, from a middleware point of view, whether you are talking to a file system or a virtual machine card, because there is just one card edge. So, for reasons of interoperability, this is very important. So, the real drivers behind the design of part 3, the PIV-2 endpoint, are that the requirements of PIV since it is a fairly narrow application domain in terms of interoperability are stronger or higher interoperability requirements than we were trying to address with the previous GSC Interoperability Specification. Also, some of the things that we have done here helped to future proof the PIV architecture overall, because we do not, for example, want to be having to change middleware every time, you know, a new card type comes out.

GSCIS was able to accommodate file system and virtual machine cards, but lets say a completely different type of Smart Card comes out in a year, you do not want to have to rewrite your middleware to recognize that. So, technology neutrality is extremely important for future proofing this architecture.

The data model is the same, as I have said several times. The only difference really, as you move from the transition spec in part 2 to part 3, the end-point specification, is that we are using essentially a different labeling mechanism for retrieving the data objects in the data model. We are using, what I call, BER TLV tags rather than the old 2-byte GSC identifiers, but aside from that, internally, the data model is still exactly the same.

One of the issues that is always surprisingly difficult in the Smart Card world is how you name things, how you keep collisions from happening across name spaces. You would think that things are simple as file 2 byte, 3 byte, and 1 byte file identifiers would not be a big deal, but they turn out to be. So, we are actually going to be managing three name spaces for the PIV2 end-point specification. The first one we will be using is the international OID or object identifier name space. NIST owns something called the computer security object register of the OID name space and we are using these OIDs to refer to the PIV credential elements at the higher level interface. I will talk a little bit more about this in a minute, but the equivalent of our old basic services interface in GSCIS. Then, also you need to have an application identifier or AID for the PIV application that resides on the card. That is actually composed of something called a RID, which is fixed. It is sort of the root and then PIX or proprietary identifier extensions. I always forget what PIX means. Anyway, so that is something else that NIST will have to manage. We have not published the PIV RID yet because we have not received it, but that should happen within the next few weeks. Then, of course, we also need to manage the actual tags that are used to refer to the data objects, the BER-TLV tags that I mentioned earlier. So, we are working right now on a publication technical report, technical note, on name space management to explain how we are doing this in the PIV domain.

The PIV card application, of course, has an AID, as I mentioned, that will have this RID that we will publish. It is really fairly straightforward in terms of the security model. There is a set of access control rules that are applied to the credential element objects on the card, say for example, you might have to submit a PIN before the card will allow you to access the private key for signature generation, something like that, or another example of just reading a data object is that you have to submit a PIN actual before you can made a biometric object off the card. The PIV card application provides a fairly streamline set actually of card edge commands. In ISO terminology, these were called APDUs or application protocol data units and these are, as I said, a unified card edge. These will be the same regardless of what the underlying card architecture and operating system are and they are also completely compliant with the ISO standards. We also have restricted the functionality of the card when it is operating in contactless mode. For those of you that do not know, PIV cards have both a contact based and contactless interface on the same card and there are certain privacy and security issues that come into play when you are essentially communicating through radiofrequency contactless type technology and one of those constraints is that you are not allowed to use an asymmetric key on the card that is PIN protected over the contactless interface, whereas you are when you are operating in contact mode.

Stepping up one level from the card edge interface itself we have a higher-level client application programming interface, again the equivalent to our old basic surfaces interface or BSI in the GSC world. There are nine commands here and these are more or less a direct reflexion of the underlying card capabilities or card functionality.

There are really no surprises in terms of what is in this API. I did not put a _____ up here as if a view who are familiar with the old BSI, you know, this look very similar. One of the big difference is though between the PIV2 endpoint middleware and the GSC middleware is that the PIV2 middleware can be much, much simpler in terms of design because the GSC middleware was designed to do this mapping of different card commands and since we no longer have different cards with different commands, so we have to accommodate somehow abstract the differences in middleware as we did in GSC. Actually a programmer at NEST who is working on developing the reference implementation middleware for me, said that he figures the programming time in complexity of the PIV2 endpoint middleware is about 10-15% that of the older GSC middleware.

Publishing standards in specifications is really just the beginning of a program like this. It certainly not enough to guarantee inner operability to help reduce cause and to guarantee consistency of implementation, so we are pursuing the development of a reference implementation. Its really fairly straight forward to describe if any of you have ever looked at reference implementations before, they are meant to be sort of a normative implementation of _____ standard and that is what ours will be, it will be an implementation of 800-73 part 3. The endpoints specification so, it will include the card applications and the middleware and the card applications will run in a ______ will be capable of running on real cards. We are going to make this available to the general public. We will put it up on PIV website and we right now are targeted for having the reference implementation done is June 25, I believe, so that should be we hope a great help to implement us in terms of figuring out exactly how you do some of these things at the programming level. It also will contribute to the development of the conformance test program, because for a conformance test you typically need some sort of, you know, golden rule that you can base your tests on and so hopefully the reference implementation will serve that purpose.

To wrap up on 800-73 itself it defines two inner phases, the client application interphase and the card edge interphase. It has a _____ model that its carried across from the transitions back and really even from the earlier GSCIS work. There is informative part 2 transitions back provided in 800-73. Part 3 the endpoints back is normative, in other words it is the mandatory endpoint for all agencies. So, once you have completed your phase 2 deployment you should have nothing, but endpoint cards in your population.

I am going to save 870 even though numerically it should come next, I am going to save 876 till the end since that still in _____ one slide on that. I will talk a little bit about 78, which is focusing on the cryptographic aspects of PIV and clearly _____ relies heavily on cryptographic mechanisms. Just for example, retreating a static data object from the card is not always going to meet the security requirements of a particular application, so you need to be able to do things like generate digital signatures, do cryptographic challenge response protocols and things like that.

Our crypto people have to deal with policy issues quite a bit and most of those issues have to do with how long _____ and associated keys will be usable. In other words, not likely to be broken and there has been a lot going on recently in terms of your original data encryption standard becoming outdated and triple _____ is now mandated for government use, but there is also ______ advanced encryption standard. All of those are in the symmetric key domain and then of course everything happening with PKI asymmetric cryptographic domain and right now RSA and elliptic curve are exist in standards that are pointed to not being truly a cryptologist myself, I am going to kind a breeze through this fairly quickly. I left all these slides and here they are more detailed and will be talking about, but they are here for reference.

There are a lot of time line issues involved in cryptography and as I said moving from one algorithm and one key length or set of key lengths to another and you can probably read this as well as I can, but we are moving from 80 _____ strength to 112 _______ strength in terms of key length by 2011 and our crypto people decided that they wanted to start transitioning in 2009 to guarantee that will be up to speed by 2011 and in terms of elliptic curve, lets see, I guess the idea here is to specify a strength for elliptic curve cryptography that will help to minimize transition issue. So we won't have to go through series of you know 4-5 different key lengths over some number of years.

Okay, you have already seen a little bit about the data model, which is composed of PIV credential elements and some of these will actually in essence all of these are signed for integrity purposes. There is something called a security object, actually on the slide for some reason it is called an authentication integrity object and this object is a table of hash values of the credential objects stored on the card and the table is then signed, so that provides _____, sorry Jim.

It sounds loud from up here. Anyway in this security object, I believe came from the _____. It was actually recommended by the IV, so we added that to the data model.

Okay, there is only really one asymmetric key that is required on the card. Actually the asymmetric keys always come in pair, so the PIV authentication key actually consist of a private key in an associated X5 or 9 certificate containing the public key. The private key never leaves the card, so that key is exercised functionally through the card edge interphase. The public key certificate associated with that key can be read from the card and then there are a number of other optional key pairs on the card that thoroughly because are optional in agency can choose to place those there are not. One thing that we kind of went back ______ on and had quite a bit of discussion about was the card authentication key, particularly in the contact _______ you may want to have the card engage in a cryptographic challenge response protocol without providing the user pin to the card first and this is why its called card authentication because it happens without any intervention from the user beyond the user presenting the card to verification or validation point. There is always a sort of tension over whether this should key in the contact _____ should be symmetric or asymmetric and how and whether it should be protected. So we ended up allowing the use of an optional card authentication key that could be either symmetric or asymmetric.

So really what we are saying here is the two asymmetric algorithms you are allowed to use in the PIV domain are RSA and elliptic curve with appropriate key lengths and for symmetric key cryptography you have the choice of triple _____ and AES.

Well just the point that two-key _____ is going to be faced out over time.

Next, I think I will skip over this.

Okay and this is a little bit more about the security object, but I mentioned earlier the security object is simply a way of cryptographically signing the credential elements or credential objects that are stored on a PIV Card, said you can verify their integrity of card.

Next, okay, and this is about checking the status of credentials online in real time, I guess and the scheme and FIPS 201 uses OCSP responders. Here I am a little bit out of my depth because I am not a PTI person, so I just let this one stand as it is also.

Okay, 876 moving on to the third of the special publications I am talking about today. Discuss this biometrics in the context of PIV and there is a major issue between the use of full image versus Minutia in the Biometrics World. This issue sort of laps across interoperability and privacy and even performance. I guess the full images, again I am not a biometric expert, but my understanding is that full images can provide a higher level of interoperability, but they are also larger. They take up more space on the card because they are not compressed in any way. Minutia on the other hand can be considerably smaller, but there is not a tremendous degree of interoperability in terms of handling, I guess different algorithms for compressing and creating and verifying Minutia**.** Also, there are some privacy issues or perceived privacy issues at least in terms of the fact that a full image of your fingerprint for example use your fingerprint. You can print that out and it looks like you know an inked fingerprint. Minutia are just numbers I guess and so they do not _____, they do not look like fingerprints. There has been some work done about reverse engineering Minutia of certain types to generate a full-image fingerprint or an equivalent full-image fingerprint. So that this gets pretty complicated and because of these complexities, 876 is still in draft form. It was put out for comment a few months ago, but I think there is some very heated debate going on at high levels right now about this Minutia verus full image issue. So I do not actually have a publication date that I can give you right now for 876, as I do not know how long it is going take to resolve these issues.

Next, okay, that is it from my presentation. Here are some contact informations, I think those of you who were here yesterday certainly heard Barker who is the PIV Program Manager and there in the middle and my colleague Terry _____ both the Minutia Smart Card Program Manager and also the lead person in our formal standard efforts. We have parallel efforts going on in _____ because they are not conflicting, but efforts going on with _____ and with _____. Right now that Terry is leading to push formal standardization of Smart Card interoperability and our website where you can find all these documents including the draft of 876 is listed at the bottom here and with that, I think we will hold questions until both speakers have finished, that may be the easiest way to handle this. So without further _____, I will _____ who is representing the Department of Homeland Security.

Thanks Jim, can you hear me back there. When I was informed to address the workshop, they told me that I am participating with Jim _____ and we supposed to talk about the PIV specification.

So I called him up late last week and say, Hey, Jim what are you doing. What am I supposed to do. Jim said I will cover 800-73, 76, 78 and reference implementation. Well, what does that leave me to speak about. So, literally Jim said just show up and I will do everything. No, he, he suggested we two talked about how homeland security may take a look at this specification and implement it. So, instead, instead of talking about specifics of homeland security implementation based on the lessons learned and what I have gathered supporting the DoD CAC program as well as homeland program last couple of years. I'm going to try to present you some generic way of approach on implementation. Okay. The, the homeland security and hopefully many other agencies are blessed with some former experience from the DoD common access card implementation as well as the Twig implementation by a homeland security TSA. So the, one, one approach would be to gather lessons learned and the technology being adopted and followed the suggestions of a solution suppliers of those two programs. So, in the

DoD common access card, the card profile, some of the homeland security agencies like United States Coast Guard, the enlisted person who will have DoD CAC card and I was told that the civilians who will have homeland security PIV card, there are certain degree of compatibility issue. So, it would be easier to take the card profile of DoD CAC card and card management and card issuance where the, in the DOD case, where a person is already wedded through their dear state of ways and all they have to show up with their ID and VIA approve the authority, they call it verifying officer take a look at the credentials of a soldier and immediately go ahead and one stop printing cards and downloading certificates and so on. So the soldiers can go on and use that card to _____ access for immediately. So, so that, that was okay for prior to PIV specification HSPD-12 where that the _____ described a trust chaining as Mr. Kevin Crouch talked about yesterday and the, I've thought that the Twig program contributed great deal toward the _____ process and for those of you who is participating the program should be proud of that contribution and they took a look at the enrollment at the management and CMSC integration from that program and try to emerge that together as recommended by Mr. Crouch.

So, you've seen this before a lot and I'm not going to go through this. They are just part of a diagram in appendix of _____ and also is a part of their Twig documentation also, just want to point it out that the, a trust chaining for those people that involve in sponsoring, authorizing the judication, authorize the issue card and for those issued a card need to be in separate and involve in trust chaining side. So, I went through, some details of how these PIV functional process can follow and I combined some of the experience of the homeland security and where that the current employee come through the OPM provided _____ enter the SF form 85, 86 and that finish the pre-Roman process and in Roman process, we will take capture 10 flats, go through the identity I9 form verification in the form of 2 at least one with a photo ID.

Capture the facial photo and provide the additional entry to capture the biographic information and then we go through a process called segmentation where ______ put it in to individual fingerprint image and go through a characterization process call finding two best fingers in the implementation of two indexes and if they are bad, choose the next best two fingerprints. At the same time, the EFTS for the IAFIS generated and descended to the necessary for FBI checks and also uniqueness checks also. For those two fingerprint characterize sent to the template generation and apply a standard and see the profile and generate initial or other templates. Then upon the authorization of the adjudication officer, those packages so called enrollment package including the template is sent to card management system and where an centralize processing where card production and the card activation is a two separate process that the following process can be made in the case of once stop issue once card production, and card activation can be done combined in one place and then cards are sent to relying party and the physical access and logical access relying party can authorize the usage of that according to the authentication level of PIV card. So that would be some generic process and be discovered.

So, how do we put all this processes into a system configuration and we can do a major three categories one so called identity management system over here if I can do that, and then a card management and production system and then there is a physical access control system. Those are the three major point of architect, and since the PIV card sort of dictates the world of logical access and physical access together it will be nice to have both card management and physical access and infact identity management also under same network of agent CIT network and probably use the device like active directory for authentication of the user. So normally the applicant applies it and they will create a some kind of HR record beginning of the security create this record and the identity management system will take that and invite the individuals to come into our involvement workstation, and capture the process that I described in previous ride. We will pass that on to a card management through a some set of an API, I call a life cycle management API or notification FEI and then card management system will be using the certificate authority and issue the card through a card issue on workstation issued a PIV card. Now, before the process is handed over to the card management side. Once the office of security determines that this applicant is qualified or adjudicated then we will let the CIO side or people know, so the network administrator will create a E-mail address or unique personal number and that will be included in to a package, so that when the PIV card is issued, they can get to a logical access right away with that using the UP and in a Microsoft environment, but probably similar process can be handled in other operating system. Once when the card goes into the usage life cycle and officer security or some authorized individual need to start a revocation process and we will go through the system that provide by identity management system and will make an entry toward _____ soft system and that will be sent to a physical access control system and as well as the card management to make that entry into CRL so that the certificate will be revoked. So this is a very level architecture and I think this is generic enough for those agencies that already has infrastructure or starting off can refresh these. I added a little _____ adapter here because of the traditionally physical access control system has been pretty much vertically implemented, never need to really integrated with IT infrastructure. Need to come up with a generic way of issuance and revocation information can be passed to PA packs and so we came up with an idea of some kind of a staging database, so that once that is identity management system sends issuance formation or revocation information up there, and then we will come through a some kind of a generic open IT concept, and all the packs can be incorporated using that. Also in the case of issuing the card, the implementer may have an option to have the IT side of card management to issue the card or he can even allow have physical access control side to inner phase with the card management and issue the card there. So, it will be nice to have some kind of generic _____ API, so that once the program rules out and you have to handle the multitude of pax with a different issuance environment. The common issuance and component can be applied to both physical and logical side and also communicating between the identity management and card management. Some generic API call card life cycle and notification API could be used and they will allow the implementers of these agency program can pick and choose the technologies ____ suppliers based on these common API. So that is the sort of lessons learned that I came up with for last couple of years. So if I could just there to provide some kind of generic implementation plan, just like Mr. Crouch has indicated that the _____ security put together and they so called integrated product testing process and put all those stackholders together and shared the lessons _____ as far, and I have also in a process of putting a infrastructure survey for physical and logical and protrude properly respond to the pending OMB requirement by June 27. The another area is that the IDMS database so called the enrollment database, the integration of that what the existing HR or security clearance _____ database is critical, not only to take those individuals already _____ and issue the card, but we will be able to handle the new applicants coming in. After that the PIV1 the implementation combining the IDMS and CMS _____ component together, as I indicated that it will be nice to have put all that under one enterprise architecture, and this is my understanding that date is we need to be ready to issue PIV1 compliant card October 27, 2005. Then after that we have an ongoing the agency wide migration for both physical access control system and IT infrastructure unless those are available, we just cannot rule this card out. So we need to be in sink with the enterprise has Mr. Kevin Crouch indicated that he is following these foot steps of IT site of VA as well as implementation.

As Mr. Kevin Crouch indicated that he is following the footsteps of IT side of _____ as well as implementation, the rollout schedule of a PIV physical access control system of all those components, and as I said again, the it is I believe it is essential that the agencies get together and push for these open APIs as I indicated and hopefully that 2006 will be ready for PIV-II. At this point, to be compatible to DoD side, we are currently looking at the trend of satisfying transition phase of 800-73. Thank you very much.

Who is first?

Yeah, questions.

This is Thom _____.

They are going to ask fill all the questions, I think.

I am Scott _____. I am contractor to the DHS and do not know who this question would be directed toward and maybe that is part of my question, I am going to assume that not every one in this room is cryptographic or PKI expert, and I was wondering is there a guideline for PIV-II that outlines from a functional perspective? If I implement the minimum requirements of PIV-II, what can I do with it as a user? Is If I implement some optional requirements that are not requirements, but optional things, within PIV-II again what can I or can I do as a user and then are there things outside of PIV-II that might be interesting or may not be interesting to implement from a user perspective? What can or can I do with that?

Sure, I can at least try to answer that. In terms of what you what you have to do, we worked with IAB actually to develop a set of used cases that you know and attempt to formalize the the requirements and processes that are in FIPS 201, and those are provided in an appendix in 873, and of course, there is also the the raw information itself in FIPS 201 about what you what you have to do. In terms of the optional capabilities, we haven't developed used cases for those in general because they they kind of tend to branch out you know once once you go down the path for example of key management that that gets pretty complicated, and there are wide range of things you could do. It is possible that at some point in the future we might might try to get together with other agencies, maybe through the IAB and diagram out some of the optional capabilities that are available, but, for right now, those those optional capabilities are really just represented through specific functions and data objects that that are available in 873.

Jim _____ follow onto that might want to talk a bit about applications management anticipated and we talked about things like the _____, talked about things like other benefits that some of the agencies have implemented. I think that may go a little bit more toward their questions well.

Yeah, the PIV application can be implemented in in in just a single applet or application, I should say, on a card, but it is possible to have the the capabilities spread across multiple card applications and that sort of opens the door to the idea of application management, which we we have not yet addressed in the PVI framework because that was not specifically needed to support the core PIV requirements, but a lot of agencies are going to want to either use some of their existing applications on the card to provide PIV parts of the PIV functionality or turned that inside out. They may want to add other applications to a PIV card certainly that are outside the domain of of PIV itself. So again, these are these are things that I think will will have to evolve over time and this certainly hopes that that we can you know actively work to to pursue that and provide implementation guidelines and developer workshops, and and there are a lot of people we can work with, the Smart Card Alliance and the IAB and other organizations to do that, okay.

I will make 'em up if they don't.

Aa-ha, this is good.

Hello Jim.

Good afternoon Jim. I want I want to ask a question related to conformance, and we we have talked about this, so you know you know you should be unexpected to to hear these questions or question, but the motivation really behind his question just to make sure put in the right framework is the e-authentication requirements having a a two-factor authentication, we're talking about the level three and four in 863, I think is where it is. Looking at M0505 for digital signature, which says that you need to have a smart card based PKI for doing these high-confidence signatures, so in the effort of dealing with these external factors really to PIV is to provide a short-term solution that you know we can go out and implement, so, on that basis, there is a few agencies and and maybe some agencies that maybe on the brink of issuing cards to meet those requirements and and there is a motivation outside of the deadlines in the schedule that are set by the OMB to do this specific you know specific deadlines to PIV that would motivate agencies, who want to go forward this, so having said all that what I am really going to ask is that based on what products you can buy today?

There are FIPS 140 validated that would allow us to move forward and issuing a what would look like a part 1 card trying to achieve part 2 requirements. A standard 64K java card with three applets, the access control applet, the PKI applet, and the general container applet, which you know gets into the application processes just mentioned with a PIV data model. Will there be a specific conformance, configuration that you know _____, you know the migration of part 2 solution that can exist for the period of the card life cycle, so if we issue those cards over the next year, typical life cycle for a card is, we will just say, three years, so you could expect to _____ these cards over the next year that will be in the card population for you know essentially four years, and that PIV-II cards that are fully compliant would began issuing say before October 2006, and so you are looking at a a deployment where you have a mixed-card population _____ by Smart Middleware for a period of of the next four years, and and so what I am asking now with all of that background is is there going to be a specific conformance approach that will allow agencies that will not spend the first dollar, they are going to stay in a holding pattern until they can buy something they know will be accepted in a deployment activity.

Let me rephrase that you know just kidding.

Or he is kidding to ask the questions.

Yeah, I will repeat the question.

But but no I think it is an excellent question and part of that is driven by policy. It it depends as as I read it, and it it being the whole PIV universe does have stance right now, so I could be wrong, but as I read it, agencies will be allowed to have transition cards; however, those are defined. We have one definition of those in part 2 obviously that is _____ from GSC, but agencies will be allowed to have those transition cards in their population up until the end of their phase 2 deployment and that phase 2 deployment again as I understand it that actually the end date for that may differ from agency to agency, but I am starting to get into policy territory, so I am just going to leave it at that. Anyway, and in in addition, my understanding is that agencies are expected to have completed full deployment of PIV endpoint cards by the end of their their phase 2 you know whatever date might be for a given agency, and I think what you are getting at is that there there will probably be a population of cards that up until that point have have served as PIV cards that up until that point have served as PIV cards, _____ these transitional cards that will still be around at the end of each agency's phase II and the question is sort of if they still have a year or two of useful life, what happens. Now, the sort of directing answer is, if my understanding is correct and agencies are to have deployed PIV2 end point cards fully by the end of their phase 2, then those other cards would not continue to live as PIV cards beyond that deadline. So that is my understanding. However, you know how much of a problem that would be, depends on when you deploy your cards of course, because if people are going to be deploying cards like, let us say this summer, _____ it does not roll out, there probably won't be end point card product available by this summer, certainly not certified end-point cards. So if you start your rollout of the end-point cards in a bit over a year from now, year and a half, whatever the date is and you have for example two years for your phase II rollout. You would actually be within that three-year life span of the cards that you had rolled out this summer. So it would not necessarily be out of sink. So you asked for a kind of a complicated question and there are several aspects to it, but part of what you asked was specifically whether we envision a conformist test program of some sort that recognizes other types of cards aside from the end-point cards and again based on my understanding of the issues, we have been asked to focus all of our resources on developing the reference implementation and the conformist test program for the end-point cards because that itself is a big job and that is actually where everybody is supposed to end up. So we clearly have to have that. The transition cards are allowed during the joint phase to up until the end of that phase and I do not really have a good answer. Well, I know that right now _____ does not have the resources and is not planning to do conformist testing on cards beyond the part III end-point cards. So what that would lead to assume I guess is that, should an agency choose to pursue a transition path whether it be the part II specification or different transition path, it will be their responsibility to decide what sort of conformist testing they need to do for those transitional cards. That is probably not exactly the answer you wanted to hear, but this has to do with the biometric requirements. I have talked to my personal security office and they told me that they have not kept electronic copies or even paper copies of most of the current staffs' fingerprints and there if there is additional requirement of having a 10 _____ fingerprint profile for the PIV. Will it be required to go back and get a 10 _____ all the current employees and then institute a new requirement for new employees of a single roll in the 10_____ as a change in the procedure for security.

So the question is really whether there is an additional requirement for more process to go back and acquire the 10 _____ fingerprint from existing employees. I am hesitant to speak on that because of the political delicacy of 876 right now. My personal understanding is the answer would be yes. Jim.

Yesterday, when Tim was on the panel, I tried to answer almost the same question he asked you and at the time when I asked that question, it was not considered to be the same, but perhaps today it will be.

You have already passed the point of _____. I am sorry. I want to go back to his question you answered, but I want to boil it down to a real short question that everybody understands the answers too. Here is the question, it has been recommended that people procure technology now that is dear toward to PIV 2 end point and my personal belief is that there is nothing available that somebody could buy today that supports the SP 873 interfaces that FIPS II validated that they could be deploying by October 2005 that meets the PIV2 requirements and yet people have been encouraged to do that and for the audience your belief is to whether that technology is preferable today?

That is an easy one Ric. There is actually a panel on implementation issues I think coming up right after this one, but in a nutshell, I think the 873 requirements really talk about the card edge. They do not talk about the internals of the card really at all. I think it is such a simple interface and such a relatively simple set of functionalities that it seems to me fairly straightforward to implement on a programable card like a Java card for example or a basic card or something. It is a little tougher in native code because when you are talking of re-masking operating systems and you already know all this. Because we are relying on the ISO standards for the card edge and for the reader specifications and because the metal ware is considerably simpler than GSC metal ware, I think the technical effort to develop these things is not tremendous. I think actually there are two things. One of them is certification and accreditation. FIPS validation takes awhile and we do not have a PIV2 card on the market right now that is FIPS 140 certified. So that is an issue. The second issue is it is really just one bit in a register, but 873 requires that the card platform be able to inform the card application of whether it is operating in contact or contactless mode. This is something that people have been hammering on industry for a long time to include in their card operating system, but my understanding is that capability right now is not available on any commercial card. So it is a very simple thing, but it is down below the level where you can just write an applet and make it happen that has to happen in the card operating system. So I know that vendors are working on PIV cards already and these things are going to happen, but I understand that making it by October 5th is going to be difficult.

Hi, Jim. Jim, this is actually a question for Phil, but I want to take the opportunity to complement you on the work you have done on PIV II/01 and special publications.

Thank you, it has been fine, Darrell.

I want to remember the days when you guys were getting picked on pretty heavily so and some of that was by me. So I appreciate the work you did. So thank you very much.

It hasn’t ended for us Darrell.

I know, I know Phil, you mentioned that your implementation of I guess recommendations that the pack should be integrated with the I2 networks. I was just wondering what are some of the vulnerabilities for IT networks connected to the Internet and as well as I2 networks not connected to the Internet.

I think you are hitting sort of dangerous area in my knowledge level. Whatever the current lessons learnt that I found is the physical access control system whether it is connected to the _____ or not is also an issue, but let us assume that the server of physical access control system can be connected to not only the intranet as well as the Internet. Assuming that we can build the similar firewall environment that we can do for logical access, in the case of a home line security, at least personally I feel that having a common authentication device such as the active directory whether it is in Microsoft Active ADO or LDAP and other environment is crucial and having been able to communicate from a packed server level, enterprise server level to an enterprise card management server level for not only the notification of the card issuance, but also a revocation handling is crucial. So I do believe that those two networks need to be integrated under in the case of home line security _____ network. I do not know whether I am answering your question or not, but that is the thing.

That is as good as he is going to get. We have run the time. Again we would like to thank the panel for a long _____.

Thank you.