CP-PCD-079-00.doc

<same as the Log Summary field below>

IHE Change Proposal

Tracking information:

IHE Domain	Patient Care Device
Change Proposal ID:	CP-PCD-079
Change Proposal Status:	Submitted
Date of last update:	2011.08.31
Person assigned:	John Rhoads

Change Proposal Summary information:

Security References Harmonization	
Submitter's Name(s) and e-mail address(es):	Todd Cooper <Todd@80001Experts.com> John Moehrke <John.Moehrke@med.ge.com>
Submission Date:	2011.08.31
Integration Profile(s) affected:	General
Actor(s) affected:	None
IHE Technical Framework or Supplement modified:	Include version # and date of publication
Volume(s) and Section(s) affected:	See proposed changes below

Rationale for Change:

Historically, security requirements have been deemed outside the scope of IHE PCD technical framework components, deferring to the guidelines and provisions made by the ITI domain. In various sections of the PCD technical framework and profile supplements, though, security text has been added to indicate that it is not in scope for PCD; however, there is no consistency in the language between the various PCD documents, nor is it consistent with security guidelines published by the ITI. This CP seeks to harmonize the security language used in published PCD documents and to do so in a way that is consistent with ITI profiles and guidelines.

Note: It was decided to create a single CP for multiple documents vs. multiple CPs, which would unnecessarily confuse the proposed changes.

Formulate the proposed change here, if known at time of submission

Specify what exactly should be changed. When modifying existing text, paste it into this Change Proposal and DO NOT use MS Word change tracking. Manually format all changed text to **bold** and either **underline the new text** or ~~**cross out the text to be removed**~~.

CP-PCD-079-00.doc

<same as the Log Summary field below>

Moehrke's 2011.08.08 e-mail (some might be good for the PCD Users Guide):

> The DEC profile did not include a section on Security Considerations, so it provides you no guidance. I don't have the email addresses of the current co-chairs as the wiki simply points at their web site and doesn't give me their e-mail addresses. Thus I am including two very smart members of the committee. I am glad that you are considering implementing ATNA. You have done a fine job of looking at your situation.
>
> In theory one would identify every physically distinct system and define that as their "Secure Node", thus making sure that any network communications in/out of that "Secure Node" are secure, that all accesses to protected resources (PHI) are controlled, and that all security relevant events are logged. I will break this down further.
>
> In reality though one often finds that they logically have one system. I am not sure, but it looks like your case you should consider one 'secure node' the combination of the biometric measurement device <-11073-> GW . I realize that this is not one physical device, but by logically grouping these you can simplify. This logical grouping does not relieve you of making sure that the interface inside is secure. I would still recommend the mutually-authenticated-TLS here, as it is network agnostic and thus not sensitive to changes in the wireless technology or network topology. By using mutually-authenticated-TLS you are also virtually binding these two as one.
>
> So, we now have a logical boundary around your 'secure node'. As you indicate the connections in/out of this secure node would be need to be secured. TLS is the most simple, some like the more flexible security of end-to-end Web-Services. But this flexibility brings complexity, so I tend to bring it in only when a specific customer centric use-case demands it.
>
> Second thing to focus on is 'access controls to enforce reasonable policy'. This is an often overlooked part of ATNA, it is overlooked as it has no 'transaction' but it is still important to think through. If you identify all the protected resources on the device, including PHI, is there some access control that protects access to this resource? ATNA doesn't define what those policies are, they tend to be obvious to the product developer. So, the most this means is potentially just making sure that it is clear that access controls are in place.
>
> Third thing is the security audit logging. The informative list of security events that should be logged is found in the ITI Technical Framework, Volume 2a, Section 3.20, Table 3.20.6-1. Clearly any other security relevant event can be logged, this table is intended to help you identify which events might happen in the context of your 'secure node'. So you just take a look at each event in the table and ask if this event happens inside your secure node. If it does, then it should be detected and logged. You are not responsible for events that don't happen inside your secure node, nor events that you can't detect.
>
> To your last question, on if there are products in the market that can receive the ATNA audit message. Yes there are, but IHE doesn't keep track of these things so it is not an easy question to answer. There is the Product Registry list of products, this shows 20 products.
>
> http://www.ihe.net/Resources/ihe_integration_statements.cfm

CP-PCD-079-00.doc

<same as the Log Summary field below>

Proposed text from ITI (Moehrke)

Security Considerations

During the Profile development there were no unusual security/privacy concerns identified. There are no mandatory security controls but the implementer is encouraged to use the underlying security and privacy profiles from ITI that are appropriate to the transports such as the Audit Trail and Node Authentication (ATNA) profile. The operational environment risk assessment, following ISO 80001, will determine the actual security and safety controls employed.

PCD TF volume 1 (final text) -

Replace Section 2.2.1 "Device Enterprise Communication" by the following:

1.1.1 Device Enterprise Communication (DEC)

The Device Enterprise Communication (DEC) profile addresses the need for consistent communication of PCD data to the enterprise. Enterprise recipients of PCD data include, but are not limited to, Clinical Decision Support applications, Clinical Data Repositories (CDRs), Electronic Medical Record applications (EMRs), and Electronic Health Records (EHRs).

The current profile does not address issues of privacy, security, and confidentiality associated with cross-enterprise communication of PCD data. The assumption is made that the DEC profile is implemented in a single enterprise on a secure network. These aspects are on the IHE PCD roadmap for subsequent years.

The current profile does not address use cases and transactions associated with either open loop or closed loop control of patient care devices. Real-time data such as alarms and alerts, waveforms (ECG, EEG, etc.) is currently not addressed.

PCD TF-1 (final text) -

Replace Section 5.4 (PIV) "Integration Profile Safety and Security Considerations" by the following:

1.2 Integration Profile Safety and Security Considerations

This profile relies on the BCMA system to verify the clinician and patient, as well as the correct medication and infusion parameters, prior to initiating the Communicate Infusion Order transaction.

Although the profile provides infusion settings for an infusion pump, the infusion is not started automatically. The clinician must always verify all settings and start the infusion directly on the pump.

PCD TF volume 1 (final text) -

Replace Section 6.6 "IDCO Security Considerations" by the following:

1.3 IDCO Security Considerations

This profile does not require the use of ATNA. There are several implementation models for this profile that do not require transmission of data over public networks including intra-institutional, VPN, etc. However, when public networks are used, ATNA is one option for secure transport over those networks. It is recommended that the Implantable Device – Cardiac – Reporter actor be grouped with the Secure Node actor of the ATNA Profile to secure communications for remote follow-ups if data is sent across an un-trusted network.

PCD TF volume 2 (final text) -

Replace Section 3.9.5 (IDCO PCD-09) "Security Considerations" by the following:

1.3.1 Security Considerations

This profile does not require the use of ATNA. There are several implementation models for this profile that do not require transmission of data over public networks including intra-institutional, VPN, etc. However, when public networks are used, ATNA is one option for secure transport over those networks. It is recommended that the Implantable Device – Cardiac – Reporter actor be grouped with the Secure Node actor of the ATNA Profile to secure communications for remote follow-ups if data is sent across an un-trusted network.

PCD User Handbook (2011 Edition)

Add the following section after Section X.X:

[We should add something to the User Handbook regarding security & pointing to ITI]

PCD ACM Profile Supplement volume 1 -

Replace Section X.4 "ACM Security Considerations" by the following:

X.4 ACM Security Considerations

This profile does not impose specific requirements for authentication, encryption, or auditing, leaving these matters to site-specific policy or agreement.

PCD ACM Profile Supplement volume 2 -

Replace Section 3.Y.4.1.6 (ACM PCD-04) "Security Considerations" by the following:

<same as the Log Summary field below>

3.Y.4.1.6 Security Considerations

This profile does not impose specific requirements for authentication, encryption, or auditing, leaving these matters to site-specific policy or agreement.

PCD ACM Profile Supplement volume 2 -

Replace Section 3.Y+1.4.1.6 (ACM PCD-05) "Security Considerations" by the following:

3.Y+1.4.1.6 Security Considerations

This profile does not impose specific requirements for authentication, encryption, or auditing, leaving these matters to site-specific policy or agreement.

PCD ACM Profile Supplement volume 2 -

Replace Section 3.Y+2.4.1.6 (ACM PCD-06) "Security Considerations" by the following:

3.Y+2.4.1.6 Security Considerations

This profile while utilizing communication capabilities supportive of authentication, encryption, or auditing, does not impose specific requirements leaving these matters to site-specific policy or agreement.

PCD ACM Profile Supplement volume 2 -

Replace Section 3.Y+3.4.1.6 (ACM PCD-07) "Security Considerations" by the following:

3.Y+3.4.1.6 Security Considerations

This profile while utilizing communication capabilities supportive of authentication, encryption, or auditing, does not impose specific requirements leaving these matters to site-specific policy or agreement.

PCD WCM Profile Supplement volume 1 -

Replace Section X.6 "WCM Security Considerations" by the following:

X.6 WCM Security Considerations

This profile does not impose specific requirements for authentication, encryption, or auditing, leaving these matters to site-specific policy or agreement.

PCD IPEC Profile Supplement volume 1 -

Replace Section X.5 "IPEC Security Considerations" by the following:

<same as the Log Summary field below>

X.5 IPEC Security Considerations

The IPEC profile does not address issues of privacy, security, and confidentiality associated with cross-enterprise communication of PCD data. The assumption is made that the IPEC profile is implemented in a single enterprise on a secure network.