1. 关于DICOM的安全机制：

DICOM标准中是没有给出安全策略的，但会提供机制来实现安全策略，比如说为安全策略的实施提供足够的信息。

1. 关于System Management Profile：

这个是用于给Dicom系统自动化配置的。

1. 关于Secure and System Management Profile

这个就是在DICOM的官方说明给出的一系列关于安全管理的方案，每个方案官方文档都会给出需要遵从某些规则，如果某应用遵从了某个方案，在其CS应该列出及给予说明。

1. Secure Use Profiles
2. Secure Transport Connection Profiles
3. Digital Signature Profile
4. Media Storage Security Profiles
5. Network Address Management Profiles
6. Time Synchronization Profiles
7. Application Configuration Management Profiles
8. Audit Trail Profiles
9. 下面只讲dcm4che支持的一些Profile：

1.Secure Transport Connection Profiles

（1）主要是保证数据传输过程中的安全，可以支持TLS1.0，TLS1.1和TLS1.2（建议使用）

TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA

TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA

（2）除了DIMSE传输加密外，HL7 v2和HTTP传输也支持TLS，可以配置相应的端口。

（3）秘钥和证书的格式主要是JKS(Java Key Store)，或者可用其它一些格式。

2. Network Address Management Profiles

dcm4che可以作为DHCP Client和DNS Client。

3. Time Synchronization Profiles

dcm4che可以作为DHCP Client和NTP Client。

4. Application Configuration Management Profiles

dcm4che可以作为LDAP client。

就是说不同的LDAP服务器可以作为dcm4che后端来使用，dcm4che作为client调用即可，如果有这个Profile的DICOM应用甚至可以共享dcm4che的LDAP服务器。

5.Audit Trail Profiles

(1)Audit Trail Message Format Profile

就是说dcm4che支持审计和系统日志，但这种日志的数据是按照一定格式的，可用于监控系统的健康和运行状况。

内容如：

谁在何时用何种方式处理过谁的什么医疗数据造成了什么结果

每个事件都有相应的ID。

(2) Audit Trail Message Transmission Profile - SYSLOG-TLS

就是说支持以TLS的形式传输日志或审计相关数据内容。

(3) Audit Trail Message Transmission Profile - SYSLOG-TLS

就是说支持以UDP的形式传输日志或审计相关数据内容。

6. Attribute Confidentiality Profiles

这个Profile主要是在删除Attribute和保留Attribute之间取得一个平衡。毕竟删除或修改Attribute可能会导致一些风险。

(1) Basic Application Level Confidentiality Profile

如果医院有些场景是需要对Attribute进行删除，比如说教学用或出版用需要把关于病人、Study之类涉及到隐私或无关的信息去掉，这个Profile会把之类的相关信息都删除或修改。

1. 在Association级别上的安全：
2. 可以配置根据AETitle确定是否接受请求；
3. 可以配置根据IP确定是否接受请求；
4. 对于C-MOVE，可以设置只接受某些传送到的目的地；
5. 关于Access Control ID：

对于Object接收方，可以根据源AETitle或者接收到的Study的第一个接收到的Object中任意一个DICOM Attribute设置Access Control ID。

对于Query/Retrieve操作，Object的提供者可以被设置只提供与请求源AETitle相关联的Access Control ID的Object。

1. AE可以选择隐藏被IHE IOCM Rejection Notes指定拒绝的对象。
2. 如果是对于接了dcm4che的HL7应用的话，可以配置只接收来自限定的Application and Facility names的发送者的信息。
3. 在Application级别上的安全：

可以设置一个认证服务器，会用Keycloak的OpenID Connect机制，会为RESTful和Web UI服务提供安全。