

DICOM 2014 成都研讨会

8月25日

中国·成都



保证安全

DICOM安全性



Brad Genereaux

爱克发医疗

产品经理

DICOM 27 (Web技术) 工作小组行业共同主席,



- **DICOM**基于安全传输协议
- **DICOM**文件加密
- **DICOM**内容的其他传输方式
- 安全性规范
- **DICOM** 匿名化规范

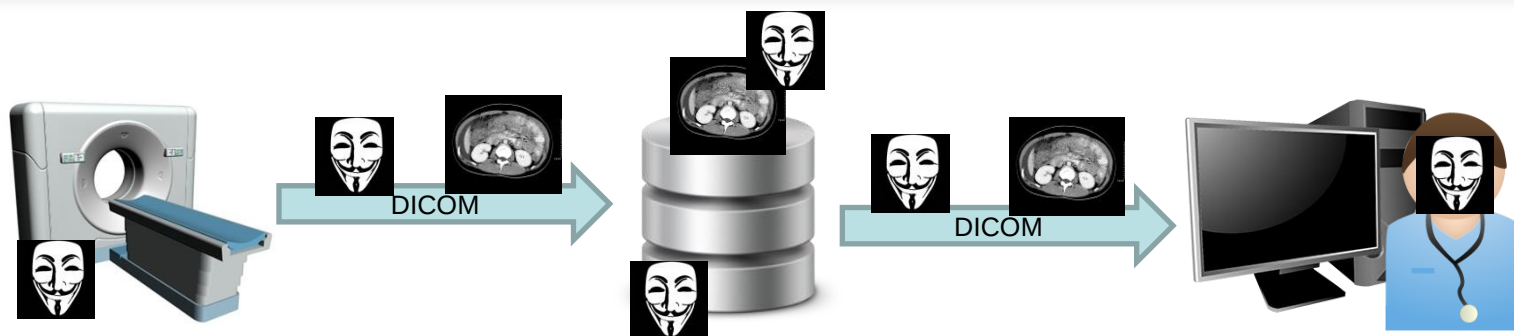
- 保护数据安全性（不允许未授权的访问）
- 保护数据完整性（不允许未授权的更改）
- 防止数据丢失（不允许未授权的删除）
- 保证数据的可用性（防止阻断服务）

如果安全性没有得到保证 将造成什么后果？

- 数据损坏或丢失
- 受害者的损失
- 民事惩罚（罚款或法律诉讼）
- 刑事处罚
- 严重的伤害甚至死亡

什么不属于安全性范畴？

- 改变参数、服务器、函数的名字，使其可读性变差
- 在发行中包含危险性功能，但在文档中没有说明



简单的工作流

- 设备传输图像进行归档
- 放射科医生请求阅读图像



:试图引起安全性问题

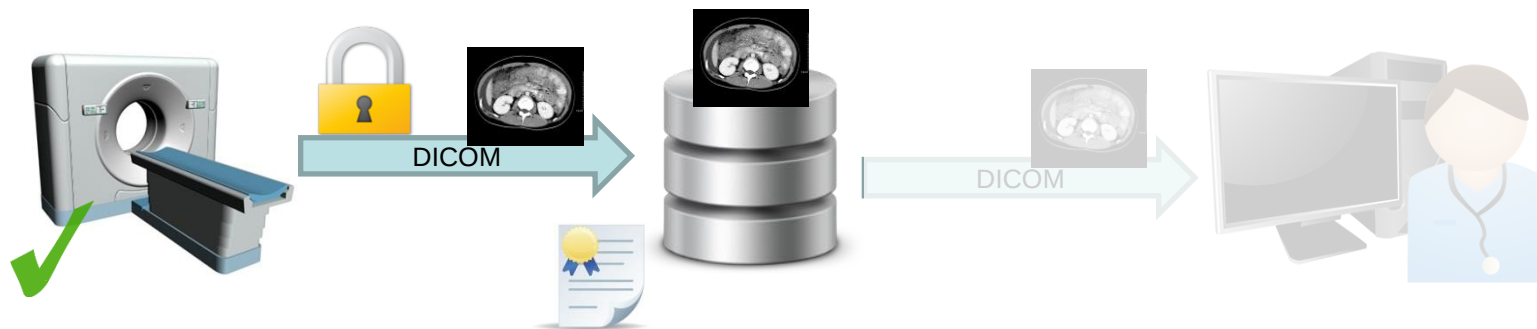
- 在标准的第 **15** 部分中定义“安全性和系统管理规范”
- 描述解决各种安全问题的方法
- 红色描述的选项在行业内使用，但是没有在 **DICOM** 标准中明确定义



谁能够看到这些影像？

- 发送影像的设备
- 接收影像的服务器
- 在设备和服务部之间网络中的任何人

DICOM – TLS 传输协议

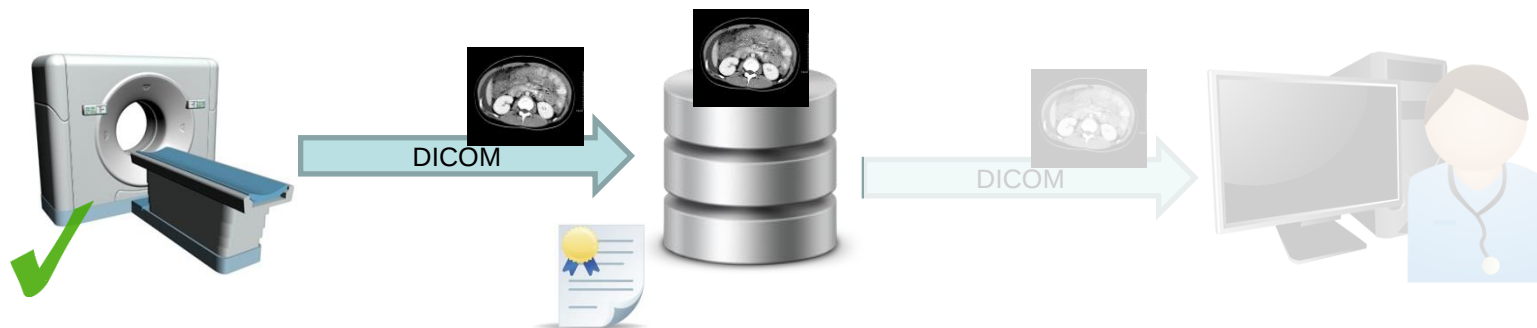


- 传输层安全加密（在标准第**15**部分**B.1**定义）
- 加密是作为安全传输协议谈判的一部分
- 传输加密是通过公共认证并通过私钥进行解密
- **网络VPN（私人虚拟网络）通道是另外一种机制**
- **DICOMweb**可以利用**HTTPS**协议（基于**TLS**传输协议）



在传输中的角色有哪些？

- 发送影像的设备
- 接收图像的服务器
- 可以替代这些角色的任何对象

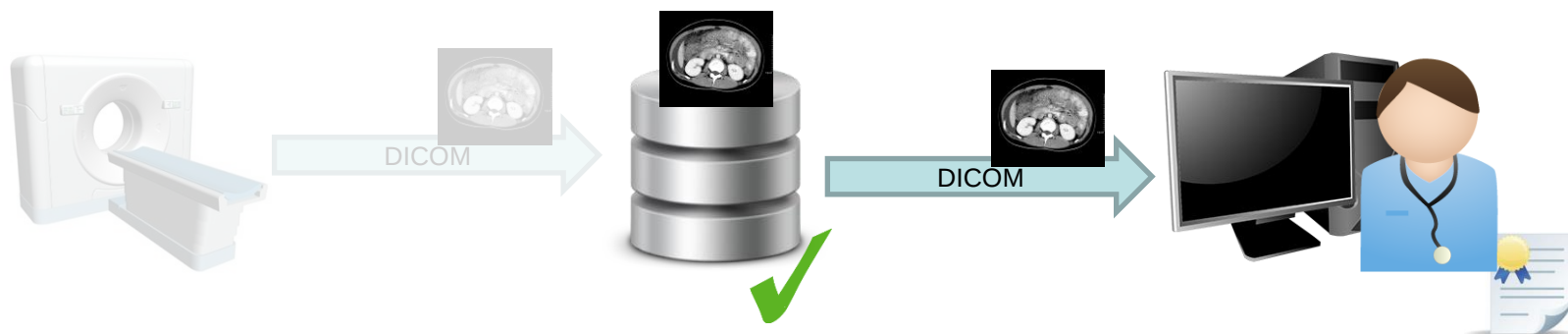


- **DICOM-TLS** 证书指定所有者的辨别信息
- 验证证书用来认证签字权
- **AE标题**是一个不太安全的选择



谁能检索图像？

- 设备由**DICOM-TLS**验证
- 用户可以检索图像
- 其他使用设备的任何人也可以检索图像



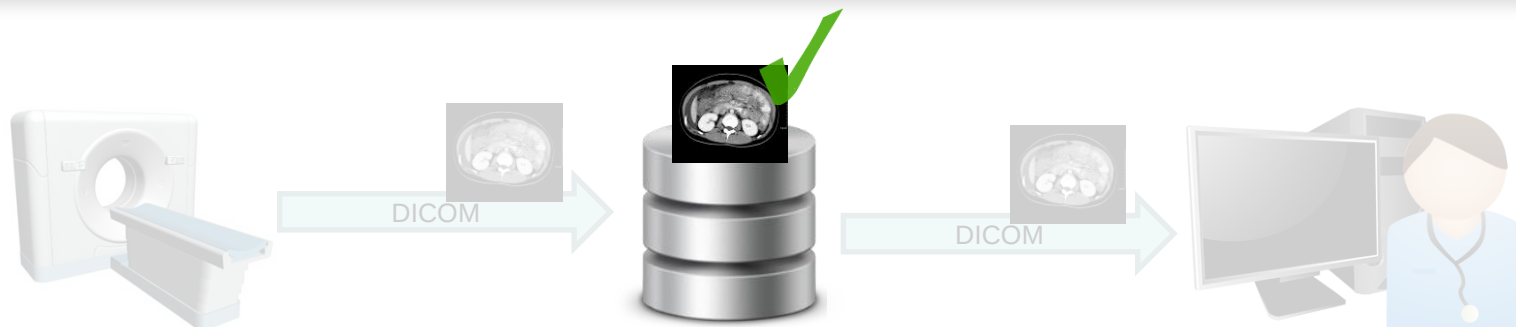
- 在标准第 **15** 部分 **4-7** 中定义
- 用户验证可以发生通过
 - 相互**TLS**认证 (每一方提供证书)
 - 协会协商期间认证 (**SAML**、**Kerberos**等)
- 在应用层级别认证用户和对图像后端作可信的调用是可选的方法

- 在标准第 **15** 部分 **A.5** 描述
- 用户标识应该在记录在审计记录中
- 身份验证、查询、访问、转换、输入/输出和删除的事件
- **DICOM** 审计标准使用在**IHE ITI ATNA** 集成规范的放射学选项



谁能确保图像是真正由成像设备所提供？

- 完成存储任务的人
- 操作存储图像的人



- **DICOM支持数字签名提供完整性检查和其他功能**
- 定义在标准第 **15** 部分 **C** 章节
- 单个字段也可以有选择的加密
- **磁盘级加密也可以用来在休眠状态保持完整性**



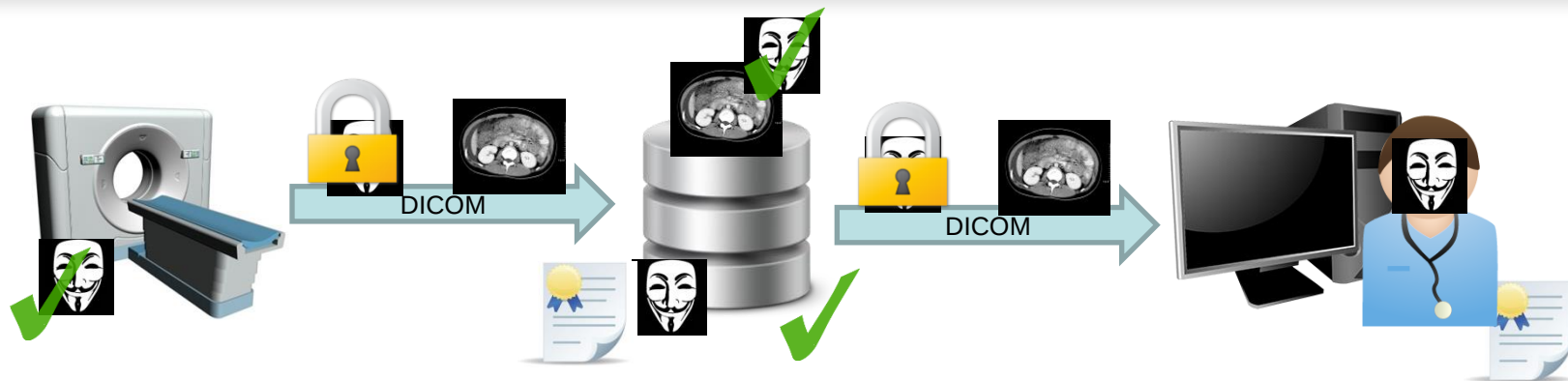
- 当DICOM传输使用物理介质(CD, DVD, USB key) 时使用
- 确保机密性、完整性和媒体的起源
- 在标准第 15 部分章节 D 定义

- 匿名化规范支持各种目的的数据保密措施
 - 临床试验
 - 教学文件
- 在标准第 **15** 部分章节 **E** 定义
- **DICOM**属性的地址移除和替换可以揭示受保护的健康信息

- **DICOM**确保一个非常广泛的身份验证和访问控制政策，但**没有**强制应用系统使用它们。
- **DICOMweb** 通过使用标准的网络技术持同样的立场。

- ✓ 在和 **DICOMweb** 交互时使用**DICOM-TLS**和**HTTPS**
- ✓ 使用适当的身份验证和授权的措施
- ✓ 使用适当的静止加密机制
- ✓ 通过管理环境、严格的身份管理、防火墙控制访问
- ✓ 在整个项目周期内，而不是项目结束后，考量安全设计

确保安全!



有问题吗? 谢谢!

图片源

- <http://echoesofhumanity.co.uk/wp-content/uploads/2014/05/photo.jpg>
- <http://icdn.pro/images/en/l/o/lock-icone-6201-128.png>
- <http://blog.getcertified4less.com/wp-content/uploads/2012/02/Certificate Icon.jpg>
- <http://fc06.deviantart.net/fs71/i/2010/223/6/4/Computer Icon by DrunkenSandwich.png>
- <http://www.clker.com/cliparts/e/2/a/d/1206574733930851359Ryan Taylor Green Tick.svg.med.png>