aycan
PACS for People

Mobile Healthcare & Teleradiology – Security Whitepaper

aycan workstation, aycan telerad, aycan mobile and Apple's iPad as DICOM image distribution enhancement for PACS environments.

ayc_mobile_healthcare_security_whitepaper_180725_sp_ds . ID54676

Table of Content

1. Executive Summary

Medical professionals want to use state-of-the-art mobile technology for their needs.
They want to send images to other physicians, hospitals or imaging centers.
But very often technical and/or bureaucratic hurdles cease such intentions.

Tablets and smartphones provide mobile access to medical information.
Mobile devices offer advantages of viewing medical images on the fly.
Their functionality is still limited by hard- and software. This new technology also introduces new questions about security and effectiveness.

Due to the characteristics of tablet technology, the diagnostic use should be limited to high contrast, low resolution medical studies like MRI, CT, US, NM and PET.
Local regulations about display technology should be followed also.

aycan mobile, an iPad App for transferring and displaying DICOM images, is used in many medical facilities for different use cases.
aycan telerad offers an almost zero-config solution for easy and secure teleradiology by using private cloud technology.

Information security regarding confidentiality, integrity, availability and accountability is ensured on a solid level and complies the current state of the technology.
It even follows German data protection law (which might be the toughest law about this topic worldwide).

2. aycan mobile

aycan mobile provides a transparent way to share DICOM images in local and also to distant networks. The DICOM images are stacked into cases (at the aycan workstation software inside the hospital/imaging center) and sent to iPads.

Users have to setup a login at the mobile.aycan.com server. This server will never store any patient data and is only used for establishing the proper connection between sender and receiver.

The existence of a new case is signalized to the iPad user through the Apple Push Notification service. After login to the aycan mobile App some meta data and thumbnails of the case are retrieved by the iPad.
If both devices (aycan mobile and aycan workstation) are logged in at the same network, they will establish a secure, encrypted channel and send the images directly to the iPad. If they are in different networks without routing, they will establish a secure, encrypted ad-hoc SSL tunnel between the devices and send the images to the iPad.

aycan mobile provides several features for displaying and basic image processing, including the comparison of two series.

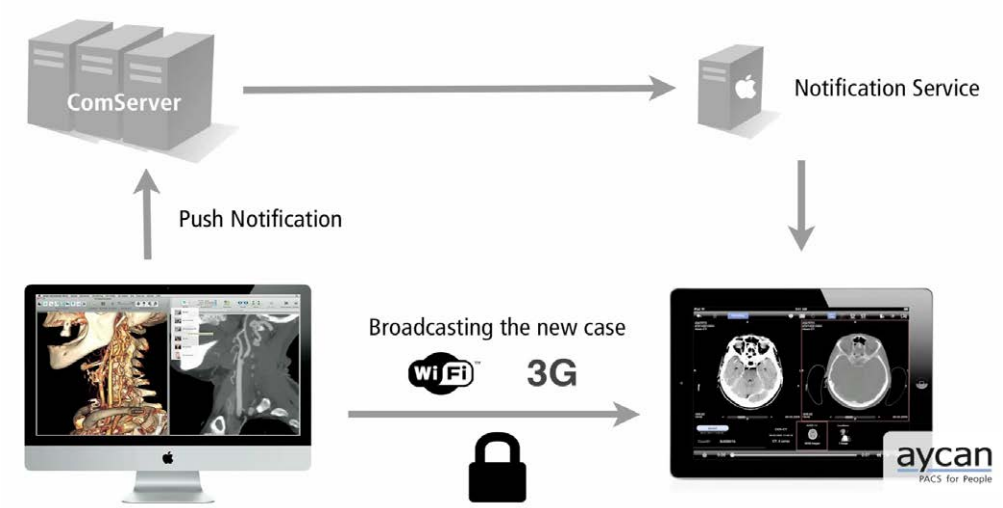

Fig. 1 aycan mobile secure workflow

3. aycan mobile use cases

There are at least four use cases for the aycan mobile system:

1. Reviewing images with patients at their bedside.
2. On-call and other remote review, interpretation, and diagnosis of radiological images.
3. Teleconsulting with colleagues.
4. Distribution of images to colleagues on-site.

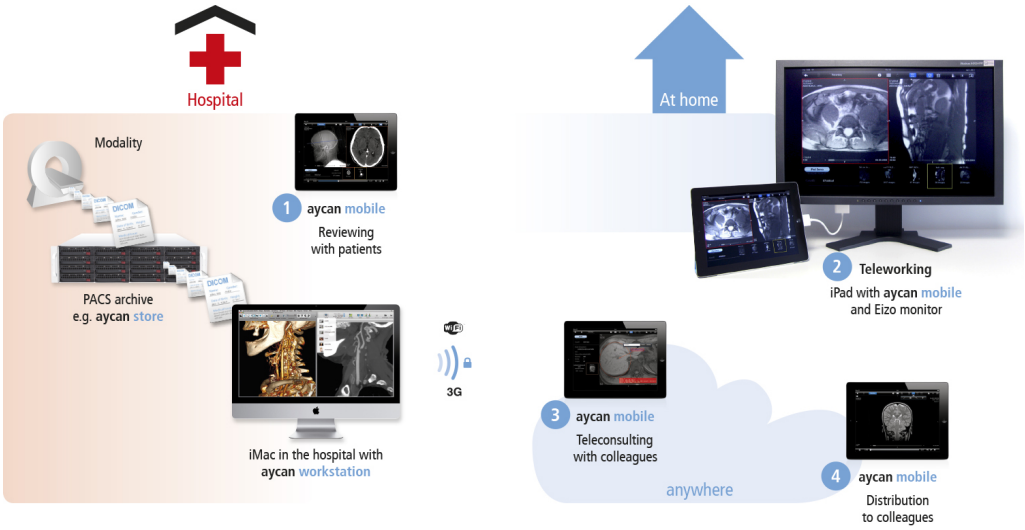

Fig. 2 aycan mobile use cases

4. aycan telerad

aycan telerad provides a transparent way to share DICOM images to distant networks. The DICOM images are stacked into cases (at the aycan workstation software inside the hospital/imaging center) and sent to other sites.

Users have to setup a login at the mobile.aycan.com server. This server will never store any patient data and is only used for establishing a secure point-to-point connection between sender and receiver.

The existence of a new case is indicated to the recipient user through a Push Notification service.

The system will establish a secure, encrypted ad-hoc SSL tunnel between the devices and send the images to the recipient's workstation.

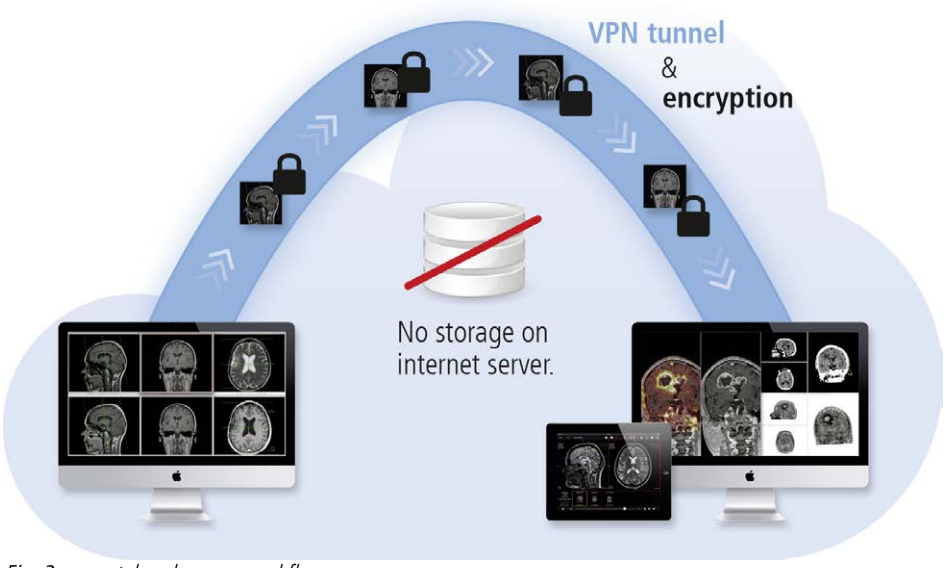

Fig. 3 aycan telerad secure workflow

5. aycan telerad use cases

There are at least three typical use cases for the aycan telerad system:

1. Connecting sites.
2. On-call and other remote review, interpretation, and diagnosis of radiological images.
3. Teleconsulting with colleagues.

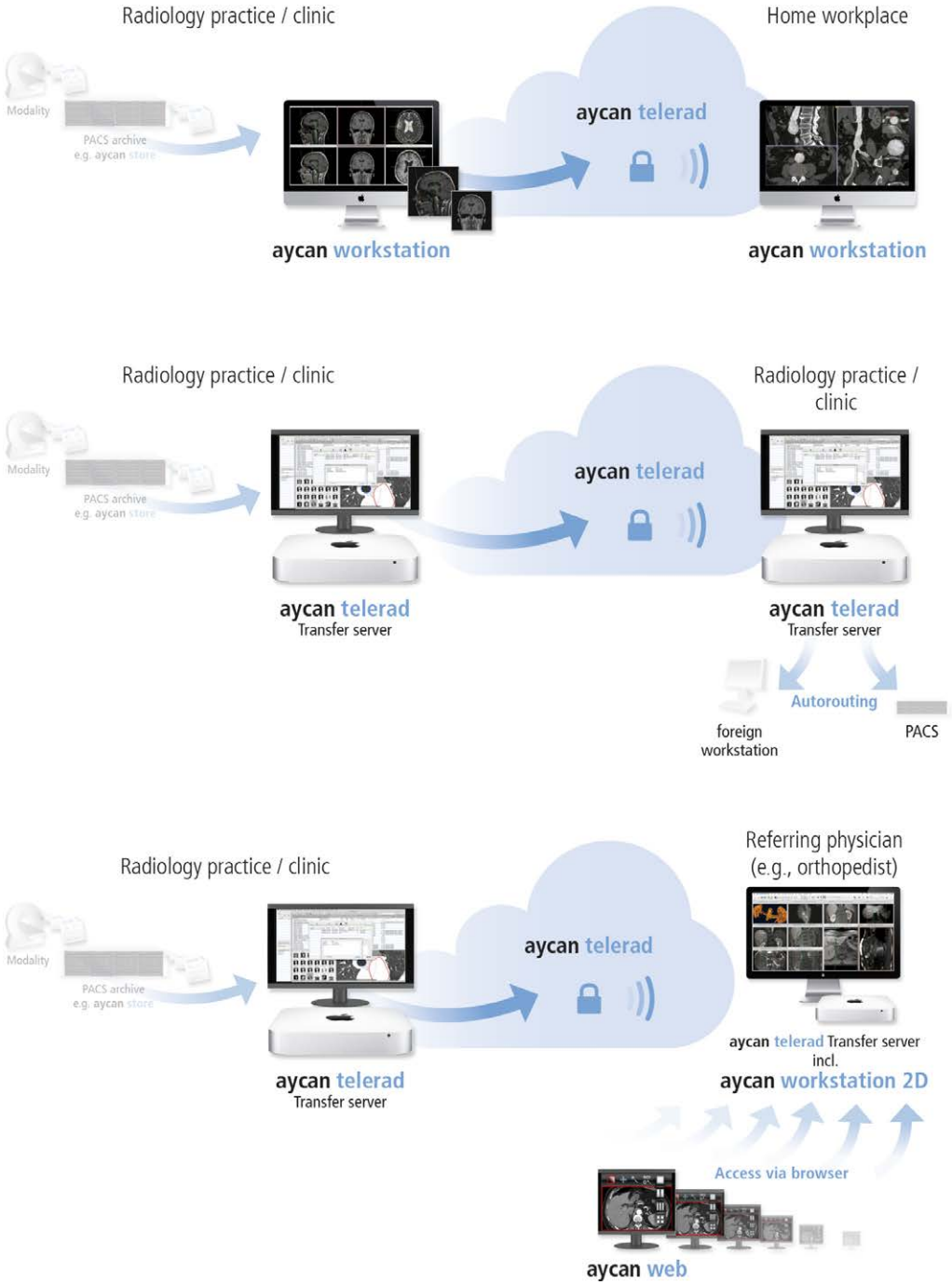

Fig. 4 aycan telerad use cases

6. Security

The overall security of the iPad and the Mac computer is documented at the Apple website, sections “iPad” > "iPad in Business" and “Mac” > “macOS” > "Security".

Topics are:
– Device Control and Protection
– Data and Runtime Protection
– Service and App Protection
– Secure Network Communication
– Secure Platform Foundation

It is recommended to setup the Apple feature ‘Remote Wipe’ in case the iPad gets lost.

Apps for iOS are reviewed by Apple before they are released for customers.
This is a benefit for the integrity and security of the software and the iPad. Currently there are no known viruses and other compromising software published for iOS.

6.1 Confidentiality

Confidentiality assures that no unauthorized users have access to the information.

There are two possible sources identified which might cause a risk regarding confidentiality:
1. Access to the information during the time when the information is transmitted to the device.
2. Access to the information while the information is on the device.

This is addressed by the following topics:
– Double encryption: Use of encrypted transmission channel (1); data is encrypted during transmission with an asymmetric encryption (2); data can only be decrypted by the recipient.
– Data is stored encrypted on the device and can be stored encrypted on the computer.
– Application and data access secured by password.
– It is recommended to send only anonymized data to the device. Anonymization of the 'Patient Name' can be used by default or switched on/off for each individual transfer.
– It is recommended to make use of remote deletion services for the device from the manufacturer of the device (see referenced ‘iOS Security – Guide’ > 'Remote Wipe').
– It is recommended to secure access the device and the computer by password.
– If a user logs into the application which keeps data for another target user at this time, the data for the other user is deleted during the login process.
– The computer should be protected physically.

The encryption is implemented in a way which doesn't even allow the device respectively the operating system manufacturer to get access to the data.

6.2 Integrity

Integrity assures that the information is correct – that is, it has not been improperly modified.

– The data is encrypted during transmission (over an encrypted channel) and during storage on the device (see 6.1 Confidentiality). From that point where the data left the source node until the data is stored on the target system and displayed on the screen, there is no possibility to alter the information at the data sets. This is because modification would imply correct decryption and correct encryption after modification, which is not possible with reasonable effort.

– The data transfer mechanism assures that incomplete or modified transmissions can be detected and that the user is notified.

– Regarding the software distribution process defined by Apple it can be assumed that only aycan is able to replace the application itself by another version. Software modifications on the device are not envisioned. Therefore unwanted software changes can be seen as precluded.

6.3 Availability

Availability suggests that the information will be available when needed.

It is in the nature of a mobile device and a teleradiology application that they have to handle the uncertainty of the transmission channel, especially if the area of mobility is not limited to a certain area where somehow controlled transmission channel conditions can be expected, like at a hospital building or campus.

– Usage at time critical scenarios is not included at the 'Intended Use' of aycan mobile and is only appropriate if the network quality is reliably in a very good state.

– To ensure to have a reliable transmission channel when needed, the user should read up on the reception conditions of a certain area before he is going to use the solution there (access to WiFi hotspots or 3G/EDGE/... network access – depending on the technique he would like and he is able to use).

– Before data deletion is executed, a prompt for confirmation must be done.

– Correct operation of the update/upgrade functionality from any previous version will be checked during the verification process.

– iOS, the operating system of the iPad, is a closed system. Users don't have access to the system. Installation of applications can be restricted by the administration capabilities of iOS.

6.4 Accountability

Accountability is the application of identification and authentication to assure that the prescribed access process is being done by an authorized user.

– Every person who wants to use the system has to have a valid user account.
  For each user account a unique user name has to be selected. It is recommended not to share user accounts but to have a dedicated account for each person that would like to use the system.

– People who would like to exchange messages or images, respectively, have to authorize each other before one is able to send data to the other.

– Each message (either only text messages or messages where image data is attached) has an unambiguous user as the sender of this message.

– Each message has one (in later versions possibly more) unambiguous user as the addressee(s) of the message.

– Access to data of a certain user is only possible after successful login.

7. Other aspects

7.1 Diagnostic use

Certain countries have specific/individual regulations about teleradiological scenarios and/or medical displays for diagnostic use. Users have to check local regulations whether the display of the iPad or the workstation is sufficient for diagnostic purposes.

The display of the iPad is a high resolution touchscreen ("Retina"), starting from 9.7" (2.048 x 1.536 pixels at 264 pixels per inch (ppi)) up to the 12.9" True Tone Display of the iPad Pro (2.732 x 2.048 pixels at 264 ppi). An external (medical) display can be connected to the older iPad 2 (1.024 x 768 pixels) by an adapter and the iPad can display 1.920 x 1.280 pixels on this external device.

Fig. 5: iPad for Diagnostic Purposes

The aycan mobile iPad App is labeled with a CE-Mark as a Medical Device Class IIa in Europe and with FDA 510(k) Clearance in the USA.
It provides a visualization correction Function (VCF) according to the DICOM GSDF curve, which is similar to a DICOM Preset medical grade display.

A touchscreen is always affected by fingerprints while usage. Users should always check the display before and while usage and clean the display when necessary.

The aycan workstation software is labeled with a CE-Mark as a Medical Device Class IIb in Europe and with FDA 510(k) Clearance in the USA.

Fig. 6: Diagnostic Workstations

7.2. Hygiene

There are third-party manufacturers who offer covers, cases and shields for the iPad which can be sanitized.

7.3. Software distribution process

According to the limited influence on the software distribution process of the device manufacturer, there is a mechanism implemented to ensure that a recall of the product in case of serious risk can be done in an effective way – independently from the software distribution process.

7.4. GDPR / Data protection

All data processing takes place exclusively in compliance with applicable data protection regulations, in particular those of the GDPR.

To use a teleradiological service with aycan mobile and aycan telerad, users must register at https://mobile.aycan.com/. This site uses TLS encryption for security reasons. This can be seen on the address line of the browser ("https: //") and on the lock symbol. As a result, data entered and transmitted can not be read by third parties.

The following personal and technical data of the user are required to carry out the teleradiological service and are therefore stored on our security server: username, password, name, date of birth, address (street, zip code, city, country), date and time of registration and last login on the server, type, duration and expiration of the subscription, name of the iPad device, date and time of the last login on the device. Voluntary information is: company / clinic / institute, telephone number, public e-mail address, contact information.

Once again it should be emphasized that at no time patient data are collected on the Internet or stored on a server!

8. References

iPad in Business – Overview
https://www.apple.com/business/products-platform/

iOS Security – Guide
https://www.apple.com/business/docs/iOS_Security_Guide.pdf

macOS Security
https://www.apple.com/macos/security/

aycan mobile user manual, section Safety Instructions

aycan workstation user manual, section Safety Instructions