Quality management, data security and data integrity in telemedicine

Gerald Weisser, MD, PhD

Associated Professor of Radiology
Head of Quality Management and IT Division
Department of Clinical Radiology and Nuclear Medicine
University Medical Centre Mannheim
University of Heidelberg, Medical School

Gerald Weisser

Consultant Radiologist in Interventional Radiology of the University Medical Center Mannheim

Full certified member of the Cardiovascular and Interventional Radiological Society of Europe CIRSE

Head of Quality Management and IT Division of the Department of Clinical Radiology and Nuclear Medicine

Vice-chairman of the IT working group @GIT of the German Board of Radiologists

Chairman of the Radiology Standards Committee, a division of the DIN German Institute of Standardization

Referenced example: Trauma-Network, Germany

Nationwide organisation of Trauma networks

- 50 regional Trauma networks
- 800 hospitals in three levels
  - Local trauma center
  - Regional trauma center
  - Supra-regional trauma center

Organisation

- German board of Orthopedic Surgeons founded a company
- AUC Academy of the Orthopedic surgery
- AUC certifies the trauma centers
- AUC started and financed a nationwide teleradiology network in 2011
- Central server architecture, clients in three levels available
  - Webviewer, Software router and hardware gateway

Content

QM overview

Guidelines

Network structures

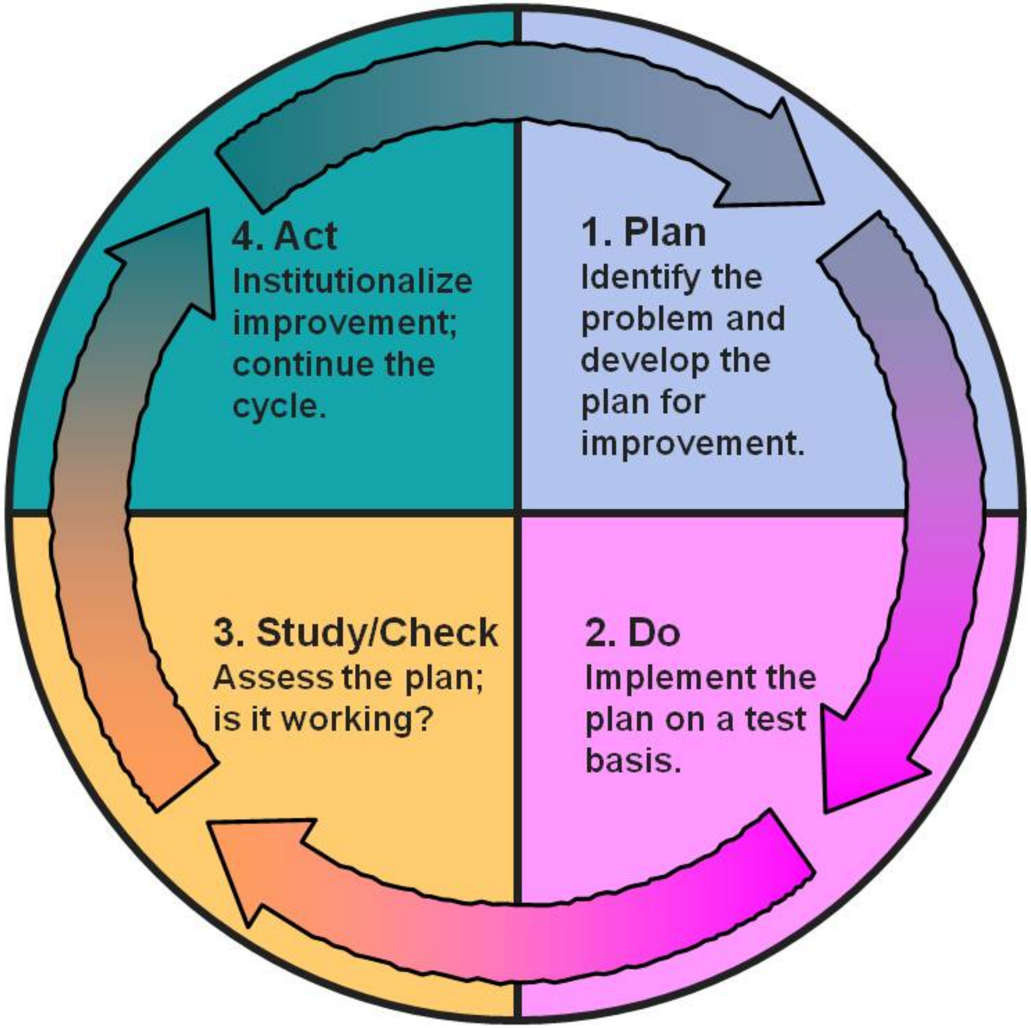
Identification and authentication

Information CIA

Exploits and attacks

Continuous QM

The Deming Wheel (or PDCA Cycle)



1. Plan
Identify the problem and develop the plan for improvement.

2. Do
Implement the plan on a test basis.

3. Study/Check
Assess the plan; is it working?

4. Act
Institutionalize improvement; continue the cycle.

Quality management in Telemedicine: PDCA

Fundamental principle is the iteration

Plan

- Carefully plan

Do

- Do it on a small sample first

Check

- Continuously check the results

Act / Adjust

- Change what's needed, then begin again

Quality management in Telemedicine: principles

Don’t get into “analysis paralysis”, the first time needs not to be perfect

Always have the 90-10 rule in mind: to reach 90% of the results it needs 10% of the efforts, to reach the 10% rest of the results you need 90% of the efforts

If you live PDCA it gives feedback and creates knowledge

“The world is drowning in information but is slow in acquisition of knowledge. There is no substitute for knowledge” Deming 1980

Quality management in Telemedicine: P

Planning a Telemedicine application

- With whom do I want to communicate ?
  - Have my partners already connections and other partners ?
  - Are there other specialties in my own hospital who want to communicate also ?
- What do I want to communicate ?
  - Images ? Other file based data ?
  - How are they stored and managed ? HIS, EPR, RIS, Lab ?
- How do I want to communicate ?
  - Real-time conferences ? Videoconference ? Screensharing ?
  - Offline or Online data transfer ? Speed of transmission needed ?
  - Timed usage for conferences ? 24/7 coverage for emergencies ?

Quality management in Telemedicine: D and C

Initial setup

- Technical setup
  - Information security and integrity, encryption standards
  - Connectivity: definition of the communication setup, line types and quality
  - General rule: never trust a company or a supplier, the marketing people always know everything and tell you that the company is able to solve every problem
- Medical setup
  - Standard operating procedures SOP
  - Medical knowledge

Continuous quality management

- Technical quality management
- Organizational management
- Medical Quality

Guidelines in telemedicine

Medical guidelines that suggest the use of telemedicine are rare

Guidelines that explain how telemedicine should be done are there

American Telemedicine Association
http://www.americantelemed.org

- Provides Guidelines for different applications of telemedicine
  - Teledermatology
  - Videoconferencing based Telepresenting
  - Ocular telehealth (Diabetic retinopathy)

Ontario Telemedicine network OTN http://otn.ca

- Provides guidelines, consent forms, clinical protocols for telemedicine
- http://www.otn.ca/en/members/resource-library (free access without registration)

Network structures in telemedicine

Network structures

- The vast majority of networks today are realized over Internet lines
- Many networks use closed VPN structures
  - Using specialized hardware (e.g. Cisco managed VPN)
  - Using central VPN-servers (can be OpenSource like OpenVPN)
  - Using direct End-to-End VPN connections e.g. via IPSec
- Alternatively
  - Webservers with encrypted connections and user authentication
  - Webservices using different protocols
    - WebDAV
    - Email

Network structures in telemedicine

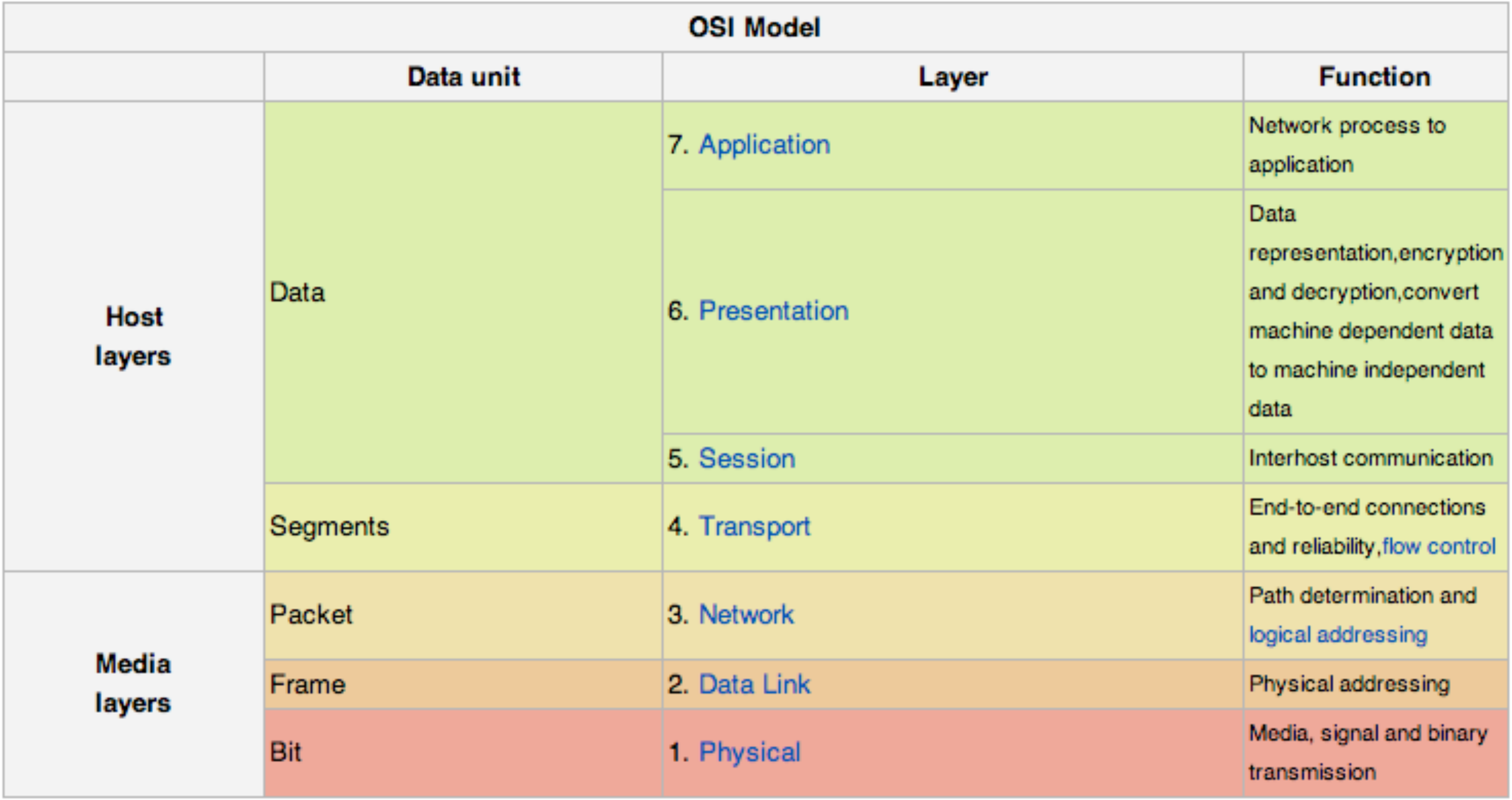
Endpoints of communication

- Mobile devices
  - Notebooks
  - Smartphones, tablets
  - Wireless devices like Bluetooth scales, blood pressure instruments
- Internet servers
- Servers and clients inside a network (firewall protected)

Communication protocols

- Bluetooth
- Wireless LAN
- Ethernet cable
- 3G, UMTS, HSDPA etc.

Communication: OSI Layer model



OSI Model

	Data unit	Layer	Function
Host layers	Data	7. Application	Network process to application
		6. Presentation	Data representation,encryption and decryption,convert machine dependent data to machine independent data
		5. Session	Interhost communication
	Segments	4. Transport	End-to-end connections and reliability,flow control
Media layers	Packet	3. Network	Path determination and logical addressing
	Frame	2. Data Link	Physical addressing
	Bit	1. Physical	Media, signal and binary transmission

OSI Layer model

Layer 1+2 Physical and Data Link Layer

- Ethernet, Bluetooth, parallel SCSI (only layer 1), FDDI
- Switches operate on these layers

Layer 3 Network Layer

- IPv4, IPv6, routing protocols, multicast group protocols
- Routers operate on this layer

Layer 4 Transport Layer

- TCP, UDP, tunneling protocols, IPsec, L2TP
- Firewalls operate on this layer

Layer 5 Session Layer

- Remote Procedure Calls RPC

Identification of devices

Network devices: MAC

- Media Access Control MAC address, physical address, Ethernet hardware address, should be worldwide unique
- Used in Ethernet, Bluetooth, WLAN
- In Virtual machines software coded

Cellphones

- International Mobile Equipment Identity IMEI number, unique to the cellphone hardware, hackers can change this (10% are not unique)
- Enter ***#06#** and it is displayed, can be banned with a blacklist
- International Mobile Subscriber Identity IMSI defines the SIM card

Internet

- IP address, is assigned by the Internet Service Provider ISP

Identification of partners in the Internet

Own IP address

- Is assigned by the Internet Service Provider ISP
- Changes after each login for private users
- Is usually stored by the ISP for a certain time, therefore an IP address can be assigned remotely to a specific user

Nameservers

- Usually a written name is used for the communication www.google.de
- The real IP address for google is 209.85.195.104
- The “phonebooks” for Internet addresses are the nameservers or DNS servers (Domain Name System)
- The nameserver is set in the network settings, multiple are possible

Identification of users: User Authentication

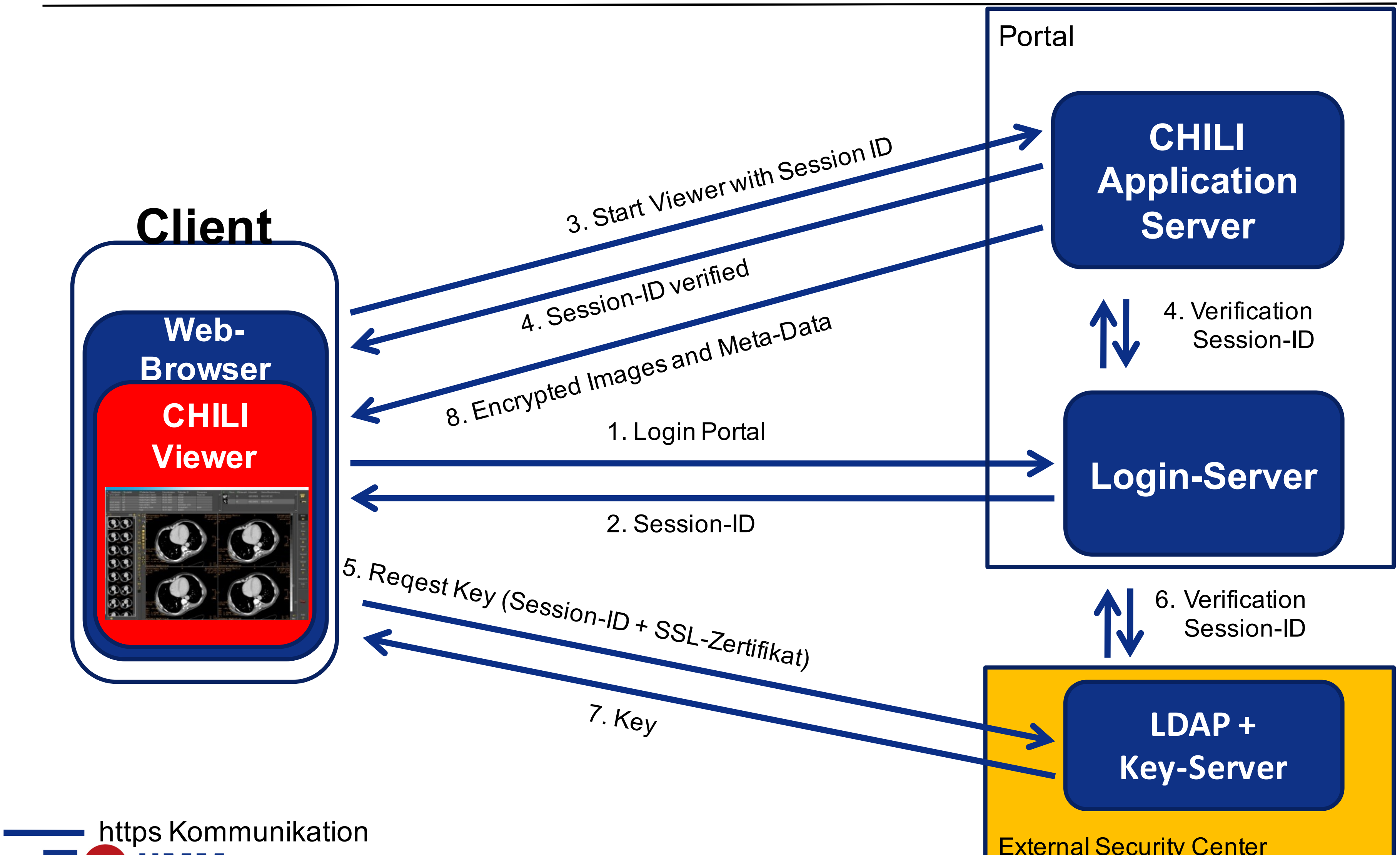
Authentication factors

- Ownership: ID card, SecurID, cellphone, passport, MAC
- Knowledge: password, PIN
- Inherence: fingerprint, retinal pattern, DNA sequence

Two-factor authentication

- In medicine two of the three factors mentioned above are needed to grant access to personalized patient data
  - ID card plus password
  - SecurID plus PIN
  - Passport plus fingerprint

Example: Trauma-Network, Security



Portal

CHILI Application Server

Login-Server

4. Verification Session-ID

Client

Web-Browser

CHILI Viewer

3. Start Viewer with Session ID

4. Session-ID verified

8. Encrypted Images and Meta-Data

1. Login Portal

2. Session-ID

5. Reqest Key (Session-ID + SSL-Zertifikat)

7. Key

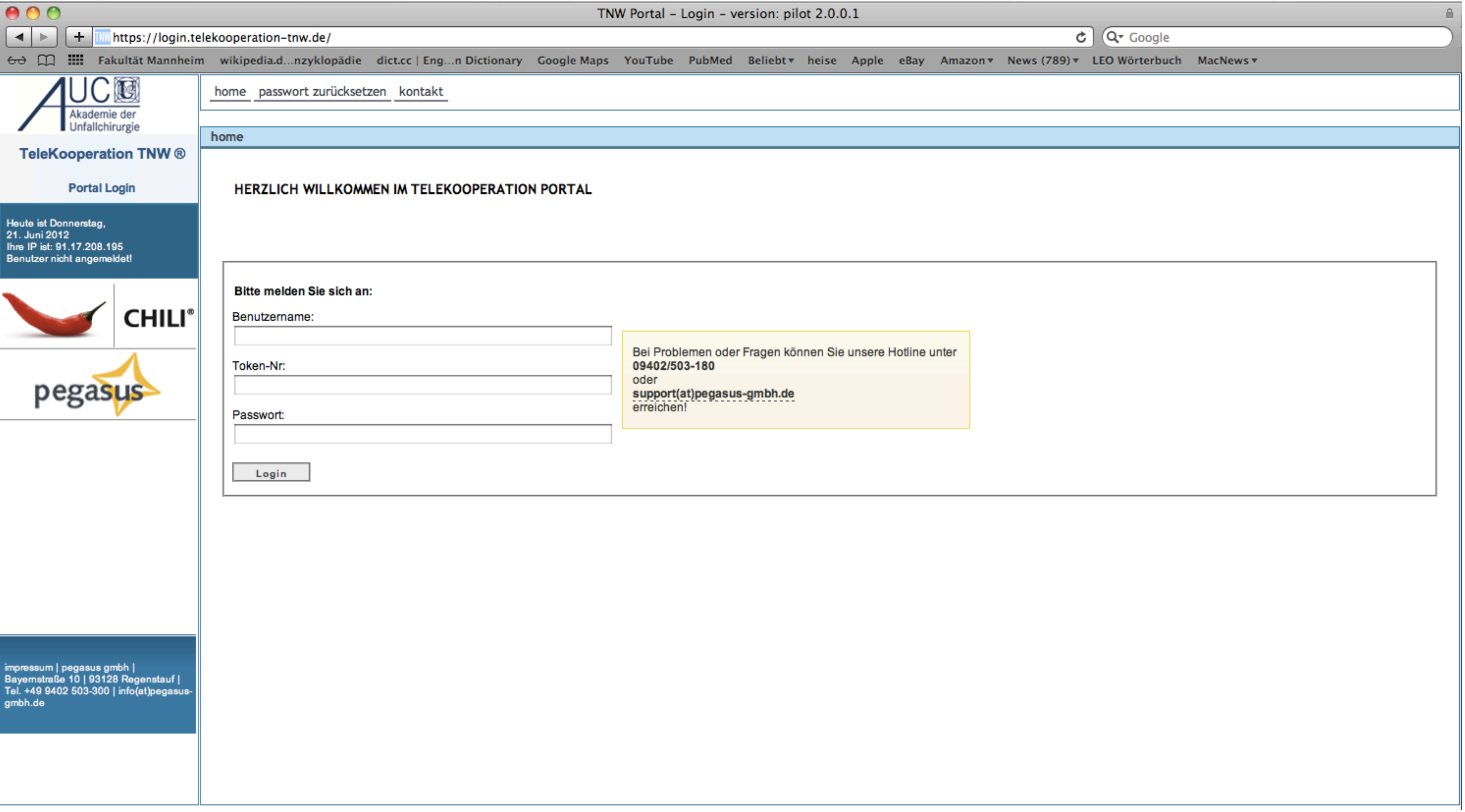
6. Verification Session-ID

LDAP + Key-Server

External Security Center

https Kommunikation

Example: Trauma-Network, Security



TeleKooperation TNW ®

Portal Login

Heute ist Donnerstag, 21. Juni 2012
Ihre IP ist: 91.17.208.195
Benutzer nicht angemeldet!

impressum | pegasus gmbh | Bayernstraße 10 | 93128 Regenstauf | Tel. +49 9402 503-300 | info(at)pegasus-gmbh.de

home passwort zurücksetzen kontakt

home

HERZLICH WILLKOMMEN IM TELEKOOPERATION PORTAL

Bitte melden Sie sich an:

Benutzername:

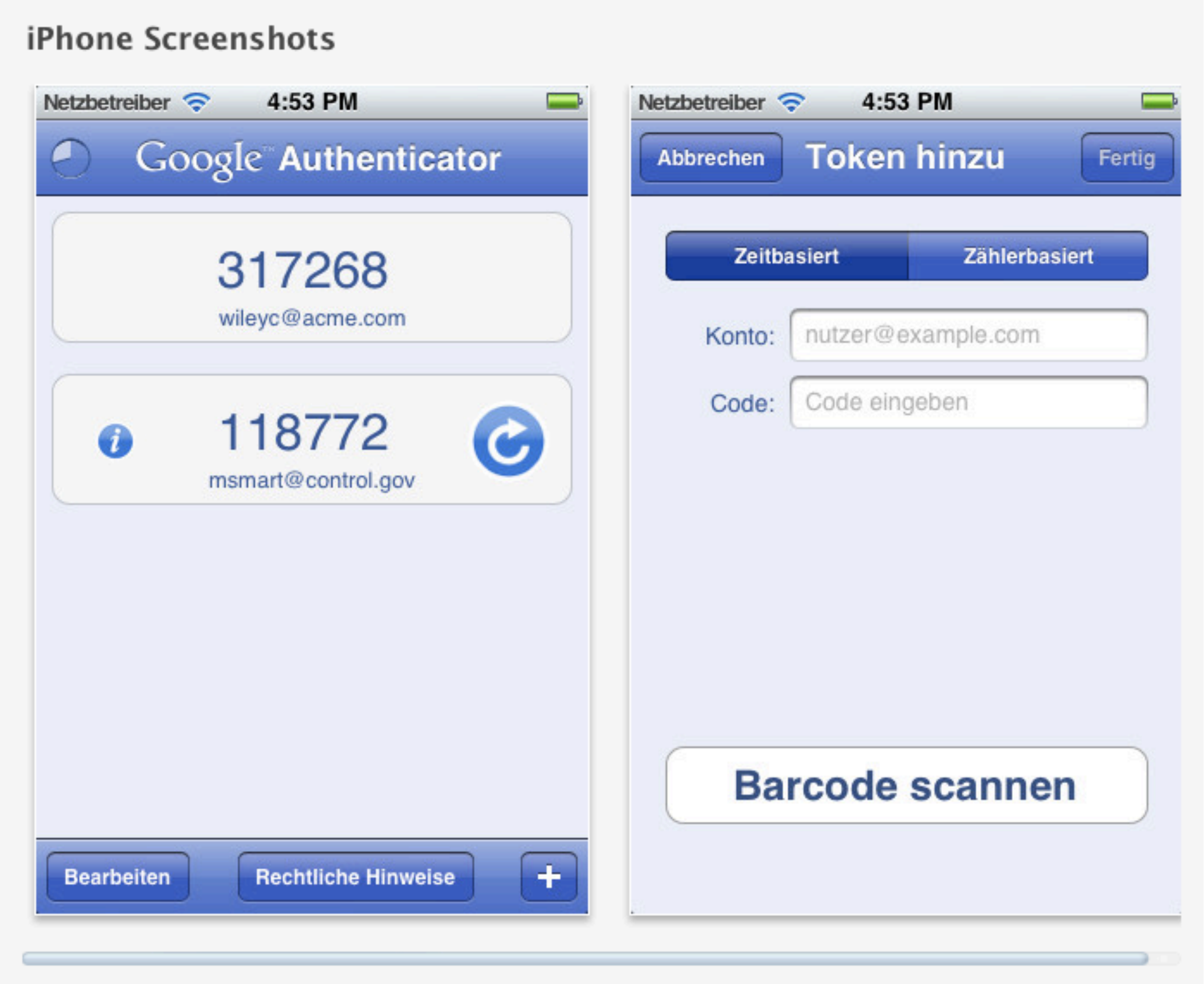
Token-Nr:

Passwort:

Login

Bei Problemen oder Fragen können Sie unsere Hotline unter **09402/503-180** oder **support(at)pegasus-gmbh.de** erreichen!

Example: Trauma-Network, Security



Example: Security of mRay viewer

Viewer used on smartphones in the UMM
www.mbits.info

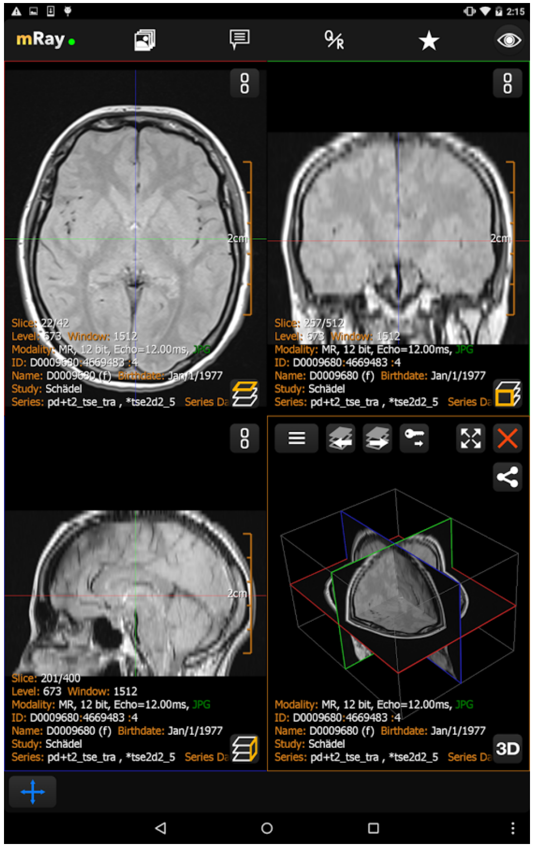
- Compatible with iOS and Android, server client
- Integrated into the DICOM archives of the UMM: send from all workstations (+700) is possible

Authentication

- User software login on the device mandatory
  - user and password, user is part of groups, patients are registered to groups
- Device needs to be registered, local token created

Data encryption

- All local files are encrypted, user switch deletes all cached files



Slice: 22/42
Level: 673 Window: 1512
Modality: MR, 12 bit, Echo=12.00ms, JPG
ID: D0009680:4669483 :4
Name: D0009680 (f) Birthdate: Jan/1/1977
Study: Schädel
Series: pd+t2_tse_tra , *tse2d2_5 Series Da

Slice: 257/512
Level: 673 Window: 1512
Modality: MR, 12 bit, Echo=12.00ms, JPG
ID: D0009680:4669483 :4
Name: D0009680 (f) Birthdate: Jan/1/1977
Study: Schädel
Series: pd+t2_tse_tra , *tse2d2_5 Series Da

Slice: 201/400
Level: 673 Window: 1512
Modality: MR, 12 bit, Echo=12.00ms, JPG
ID: D0009680:4669483 :4
Name: D0009680 (f) Birthdate: Jan/1/1977
Study: Schädel
Series: pd+t2_tse_tra , *tse2d2_5 Series Da

Modality: MR, 12 bit, Echo=12.00ms, JPG
ID: D0009680:4669483 :4
Name: D0009680 (f) Birthdate: Jan/1/1977
Study: Schädel
Series: pd+t2_tse_tra , *tse2d2_5 Series Da

Information security

Protection of information and information systems from

- Unauthorized access, use, disclosure…
- Modification, destruction

Focus on CIA

- Confidentiality (Nobody unauthorized can view)
- Integrity (Nobody unauthorized can change)
- Availability (Everybody can work)

Information availability

No single point of failure

- Cluster server for the availability of the services
- Duplicated network structures
- Fallback lines for the outgoing and incoming connections

Update management

- Testserver or complete test environment are updated first

Ideally separate systems for the same service

- Two separate archives from different vendors
- Different operating systems
- Different server room in different building (in case of fire)

Information availability: Backup and archive

Backup

- Data is copied to restore the original data after a data loss
- Can make a disaster recovery or restore corrupted data
- Can be made as a
  - Full backup (one backup can restore all)
  - Incremental backup (all backups sine last full backup needed for restore)
- Again: for crucial data multiple copies in different buildings needed
- The restore process must be tested after relevant changes of the process

Archive

- Data is not only backuped but also reassured, that the original data is unchanged (signature)
- Data history is maintained: multiple versions of files after changes

Information availability: DoS attacks

Denial of Service DoS attacks

- Very common to Internet services
- Flood of requests overload the Internet servers
  - Very often realized by Bot-nets, usually infected computers with troyans or viruses on it that can be controlled from a central instance
  - Each infected computer does produce its own requests, therefore it is not possible for the Internet server to easily differ between real requests and DoS requests, called a DDoS Distributed DoS (up to 30,000,000 bots)
- Also possible for Mailclients
  - e.g. create Mail attachments with ZIP compression and giant size after decompression

DoS attacks are often part of an extortion or a political act

To repel a DoS attack you need profound knowledge

Information integrity: Nobody can change

Digital Signatures, Keys

- For the encryption and signature of documents a signature key is needed that can be generated using specific algorithms like RSA, DSA, ElGamal etc.
- To reassure that the key is correct you need a Public Key Infrastructure PKI
- Official PKI store the keys for >30 years, each key does have a validity of 3-5 years only
  - The keylength and the used algorithms changed in the last 10 years because some algorithms were tampered and shorter keys can be cracked
- The keypair consists of a private key, that can do the signature and the corresponding public key, that can only proof the signature
- The public key is available in a keyserver to all users

Information integrity: documents

Signing of documents (digital objects)

- Using a private key and according algorithms you can sign a document and store that information within the document (pdf supports that) or as a separate file
- If a document is received you can use the corresponding public key and the signature proof algorithm
- If the proof is identical to the signature stored in the document then the document was not changed
- For longterm storage of documents you need to re-sign the documents after 3-5 years because the keys are not longer valid

Information confidentiality: Nobody can view

Access to resources

- Use two-factor authentication
- Change passwords frequently (every 4-6 weeks at least)
- Use safe passwords
  - Min 8 characters
  - Numbers and characters
  - Upper and lower case characters in unusual combination
- Make sure that you are not intercepted/eavesdropped

Personalized accounts

- In a medical environment no group accounts are allowed for personalized data access
- All procedures must be assigned to a real person for medico-legal reasons

Information confidentiality: Nobody can view

Line encryption

- No transmission of any personalized data over unencrypted public lines allowed
- In Europe double encryption (line encryption plus content encryption) is mandatory
- All Internet protocols are available in secure variants
  - https, imap4/s, pop3/s
- All (current) mobile devices support encrypted protocols

Virtual Private Network VPN

- Encrypted protocols that tunnel all other traffic through that protocol
- IPsec, OpenVPN, L2TP
- Available in all operating systems and all mobile devices
- Setup can be very complicated, known incompatibilities

Information confidentiality: VPN

Use in corporate networks

- All global companies, all larger Hospital groups do have VPNs
- Within a VPN all partners worldwide can be reached in one logical network
- Access from mobile devices to that VPN is possible worldwide over all connection techniques
- Almost always the two-factor authentication is used
  - Notebooks with built-in fingersensor
  - SecurID devices
  - Check of the ID of the mobile phone
  - Smartphone Apps like Google authenticator

Biggest problem: Exploits

What is an exploit ?

- A piece of software that takes advantage of a bug or a vulnerability of another software to gain control over resources
- Most exploits attack Internet browsers, mail programs, banking software, webservers and any other kind of software, that runs on Internet servers or other computer connected to the Internet
- Technically many exploits are based on buffer overflows
  - Computer systems do not differ between program data and user data
  - If a bug in a program can lead to storage of user data in the program area, then it can be run as a program using the access rights of the current user
- That is the reason for all the patches for IE, Firefox etc.
- An exploit can be activated by simply watching a webpage or reading an Email or even watching a picture (jpg) from a USB stick

Other problems

Man in the middle attack

- You want to connect to a server e.g. Telemedicine portal
- Somebody intercepted your system and you really log into a foreign server, that foreign server displays the user interface exactly like the real server
- You enter your data, the data for authentication is simply forwarded to the real server but also stored for illegal transactions
- You make a transfer but in reality the money is transferred to a different account

How is it done ?

- A mail was sent to you and you click in the mail link instead of your bookmarks, that link is faked
- Or worse: some troyan changed your DNS server

Consequences for system administrators

Block any port that is not needed

- USB sticks and DVD drives can have autostart functions, that can start malicious software
- Disable autostart !

Restrict Internet use (can the doctors still work ?)

- Use whitelists (only specific Internet pages are allowed)
  - That can be a lot of work for the administrators
- Block webmail providers (users will hate you !)
- Use deep inspection of the traffic to find malicious activities

Manage the local systems

- No boot from external devices
- No relevant data on the local harddisk

Why all that fuss ?

Nobody cares about my data anyway !?

- Every Hospital does have VIPs and own employees as patients
- The most interesting VIP is very often my own neighbour or my rich uncle

The system administrators always overact !?

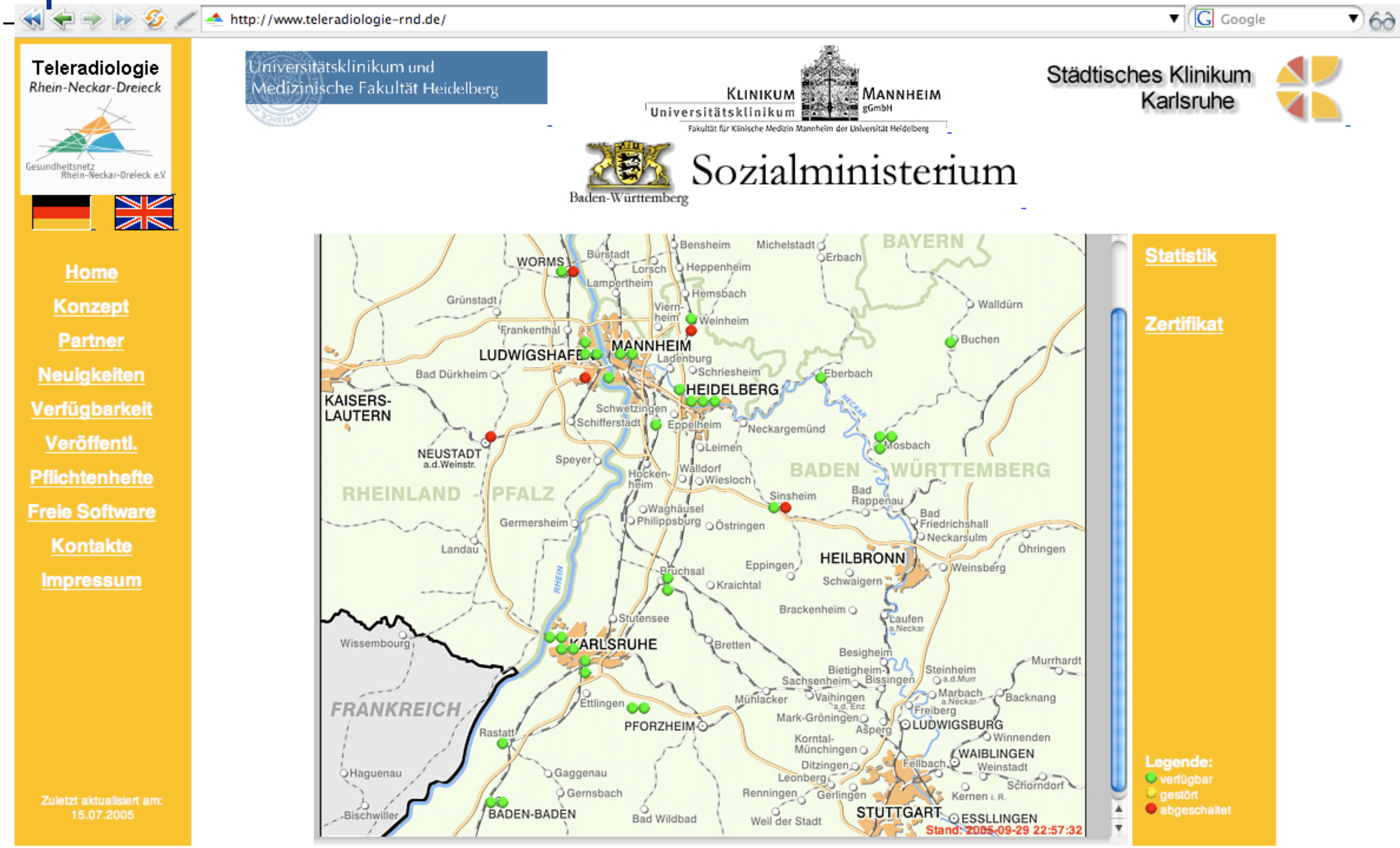
- Exploit packages can be downloaded that allow the construction of malware packages even for unexperienced users
- More than 3,000 hacker attacks per bank per year
- In a private computer connected to the Internet you can find up to 1,000 port scans per hour, that are blocked by the local firewalls

Continuous Quality management in Telemedicine

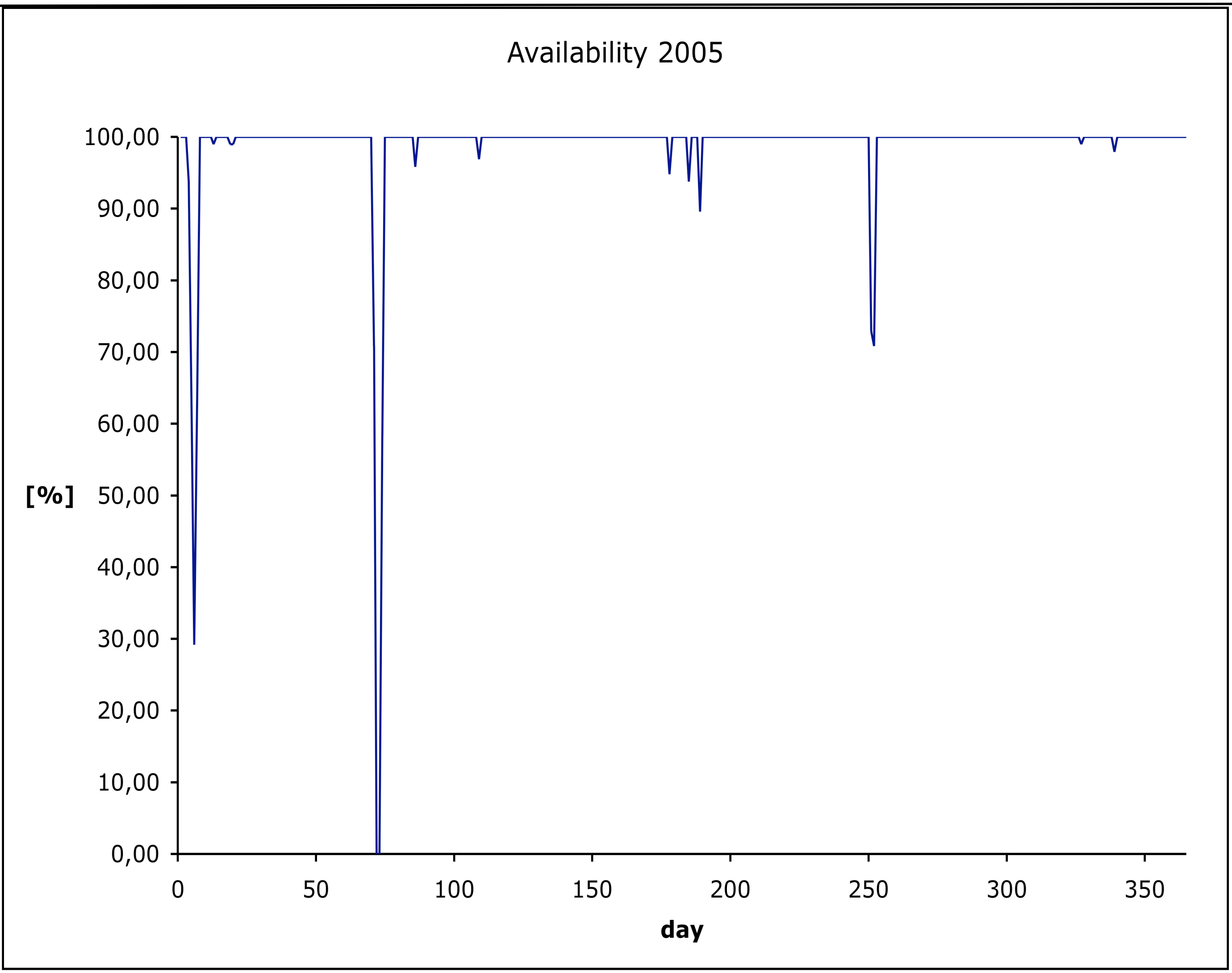
Technical quality management

- Documentation is mandatory
  - and often incomplete or missing
- Continuous check of the components involved
  - “In god we trust, all others must bring data.” W.E. Deming
  - Software like Nagios.org or Shinken-monitoring.org
  - Can check components over SNMP and any port without client
  - Bunch of other checks with installed clients
  - Overview can be displayed as a map and on a webpage
  - Make sure that somebody really reads the error messages
  - Make sure there are no useless error messages
- Regular check of the state of the art
  - Line quality, protocol enhancements, hardware enhancements
  - Security measures, new encryption standards

Uptime server



Availability of the UMM gateway



UMM UNIVERSITÄTSMEDIZIN MANNHEIM

Medizinische Fakultät Mannheim
der Universität Heidelberg

Universitätsklinikum Mannheim

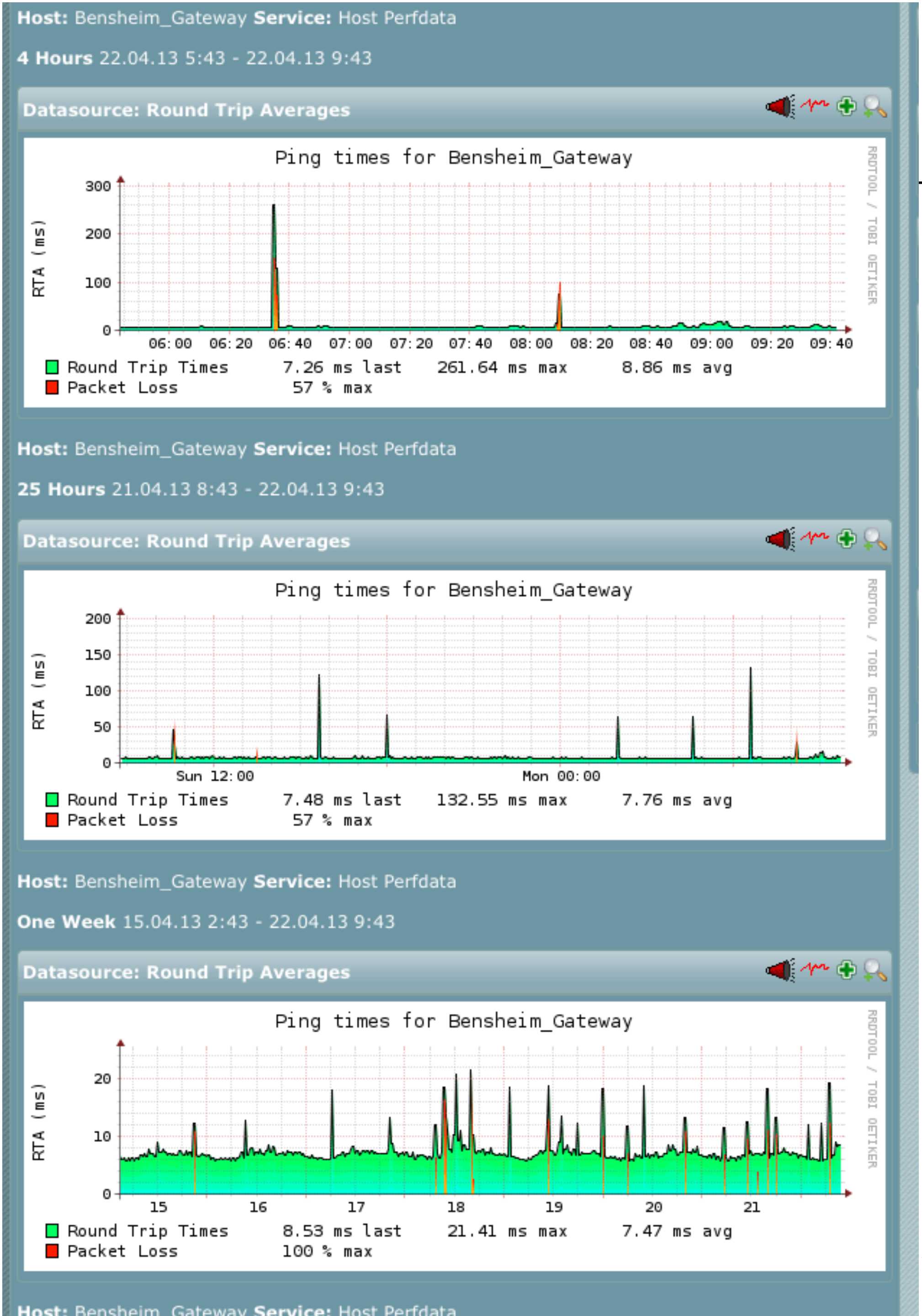
Availability of clients 2005

Institution	Beginn	Uptime (%)
KKH Baden-Baden Neu.	07.06.2005	42,50
KKH Baden-Baden Rad.	19.05.2005	50,21
KH Bruchsal	15.12.2004	96,93
RGP Bruchsal	14.07.2004	92,28
KKH Buchen	01.07.2004	99,82
Curagita Mailserver	01.01.2004	99,69
KKH Eberbach	15.12.2004	98,54
UKL Heidelberg Web.1	14.04.2005	99,92
UKL Heidelberg Web.2	14.04.2005	99,92
Diakonissenkh. Karlsruhe	01.09.2005	100,00
SKL Karlsruhe DMC.	22.09.2004	99,28
SKL Karlsruhe Neu.	22.09.2004	87,90
SKL Karlsruhe Rad.	22.09.2004	82,71
St.Vincentiuskl. Karlsruhe	15.09.2004	81,07
Kl. Karlsbad-Langenst. Neu.	13.04.2005	97,09

Institution	Beginn	Uptime (%)
Kl. Karlsbad-Langenst. Rad.	13.04.2005	94,20
Kl. Ludwigshafen Neu.	04.08.2004	97,93
Kl. Ludwigshafen Rad.	04.08.2004	97,35
Kl. Ludwigshafen Srv.	03.08.2004	99,72
St. Marienkh. Ludwigshafen	12.07.2004	84,22
Diakonie-Kh. Mannheim	23.08.2004	85,90
UKL Mannheim Rad.	01.01.2004	98,04
KKH Mosbach Rad.1	14.12.2004	97,99
KKH Mosbach Rad.2	14.12.2004	98,42
Praxis Peiss-Hering Mosbach	26.07.2004	98,81
KKH Rastatt	16.06.2005	47,36
KKH Sinsheim	14.05.2005	93,42
KKH Schwetzingen	22.06.2004	66,76
SKH Worms	26.07.2004	85,57

n=29

<80%:	4
80-97%:	10
97-98%:	4
>98%:	11



Host: Bensheim_Gateway **Service:** Host Perfdata

4 Hours 22.04.13 5:43 - 22.04.13 9:43

Datasource: Round Trip Averages

Ping times for Bensheim_Gateway

🟩 Round Trip Times 7.26 ms last 261.64 ms max 8.86 ms avg
🟥 Packet Loss 57 % max

Host: Bensheim_Gateway **Service:** Host Perfdata

25 Hours 21.04.13 8:43 - 22.04.13 9:43

Datasource: Round Trip Averages

Ping times for Bensheim_Gateway

🟩 Round Trip Times 7.48 ms last 132.55 ms max 7.76 ms avg
🟥 Packet Loss 57 % max

Host: Bensheim_Gateway **Service:** Host Perfdata

One Week 15.04.13 2:43 - 22.04.13 9:43

Datasource: Round Trip Averages

Ping times for Bensheim_Gateway

🟩 Round Trip Times 8.53 ms last 21.41 ms max 7.47 ms avg
🟥 Packet Loss 100 % max

Host: Bensheim_Gateway **Service:** Host Perfdata

Error search

- Continuous tests are best done end to end
- If an error occurs then the search starts
  - If more than one company is involved usually they blame the others
  - The better the information the easier the search
  - The worst errors are partial failures (partial in time or function)

Technical Quality management

Very often telemedicine installations are complex and involve several departments

- If several institutions (hospitals, clinics, companies) are involved then the interfaces and responsibilities must be clearly defined
- At every interface test-utilities or reference implementations should be present to ease error searches

There is the need of a person or a group of persons that know the whole process

- That can be a company or one of the employees
- This company or person must supply a complete documentation to make it possible to replace the person
- Otherwise the error management can end in an endless circle

Continuous Quality management in Telemedicine

Medical quality management

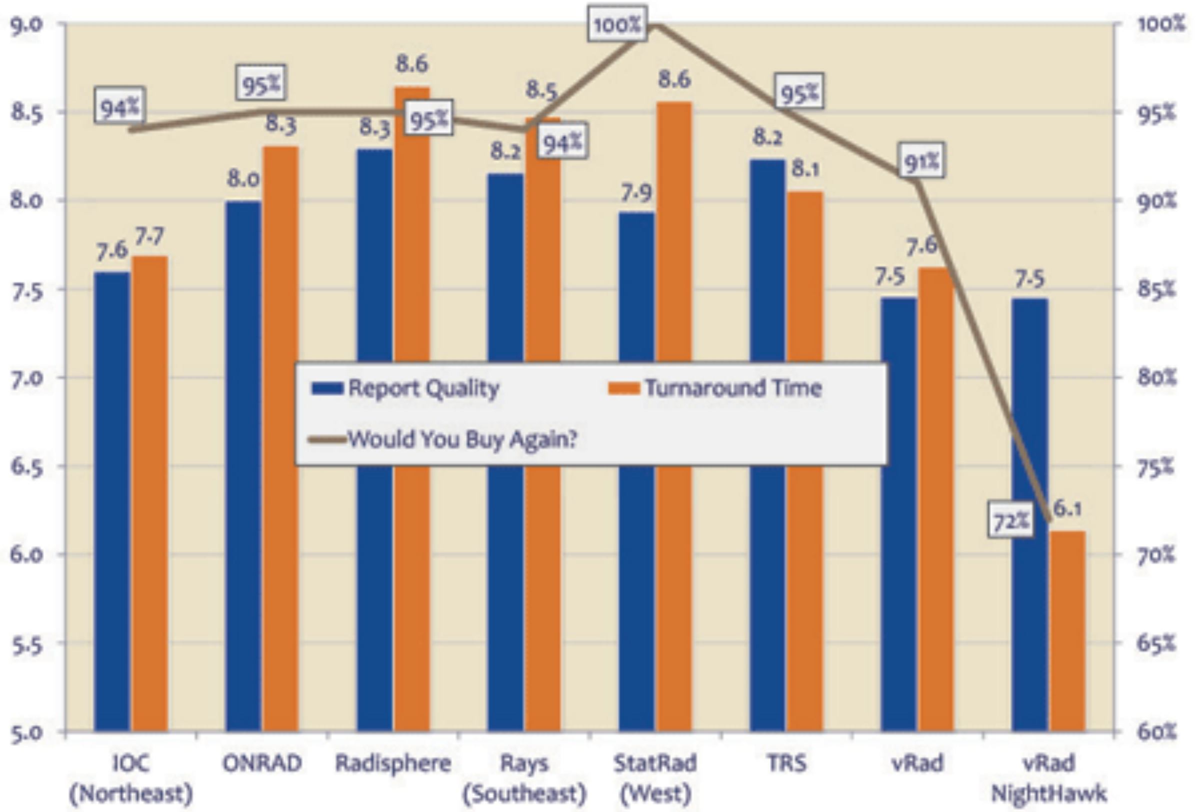
- Regular training of the staff (annual courses)
  - In the first two years of teleradiology service in RND more than 90% of the malfunctions were due to user errors
- Teaching of new employees
  - Must be structured and unavoidable
  - Best accomplished with a department handbook
- Check of the corresponding medical guidelines
  - Define the person for that task and give a deadline or it will never be done

Example: Nighthawk-Radiology Vrad.com, U.S.A.

Private teleradiology provider

- Founded by Dr. Paul Berger, 2010 merged with Virtual Radiologic
- First company that legally used overseas reporting (Australia and Switzerland)
- Provides support for 2,700 Hospitals in 50 states, 25% of all hospitals in the U.S.A.
- 400 radiologists full-time in all 50 states, 75 % former fellows
- DICOM und HL7-Integration, Internet connection
- Widely uses Software as a service and Cloud-computing
- Reporting time less than 20 min
- All Modalities, Cardiac-CT, Peer-Review

Example: Nighthawk-Radiology Vrad.com, U.S.A.



New KLAS Report Examines Effects of Recent Consolidation on Teleradiology Market and Vendor Performance October 11, 2011

Conclusion

Safe IT in telemedicine is possible

- But you have to know what you do
- And especially you have to know what you leave undone

Since a 100 % safety is not possible

- Control is mandatory
- Regular Re-Evaluation of the workflows and settings is needed
- Updates of software and hardware according to the current standards is a must

OVER 300.000 COPIES OF THIS ISSUE PRINTED AND DISTRIBUTED
RADIO
25 Cents
rations
TH
E:
R.S.
R.S.
and
el of
dards
Pyle
ote
THE 100% RADIO MAGAZINE
iPad
1:12 PM
100%
Recent Series
Anonymized