SECURE ELECTRONIC IDENTIFICATION AS A PREREQUISITE FOR REMOTE MEDICAL SERVICES

BOARD ADVISOR SECURITY EXPERT
MAREK.UJEJSKI @COIG.PL
MEDICAL TREATMENT – WHATS NEW?

• MEDICAL TREATMENT- VERY SENSITIVE ACTIVITY
• PATIENT – DOKTOR RELATIONS
• LONG TIME AGO – PEOPLE INTRODUCED TECHNOLOGY
• CONSTATLY IMPROVED FOR SEVERAL CENTURY
• BEFORE 1ST WAR – X-RAY (ROENTGEN-1895) , EKG (EINTHOVEN – 1903), BLOOD PRESSURE (SCIPIONE RIVA ROCCI-1896, KOROTKOW -1905)
• ... AND AFTER –EEG (BERGER-1929), PRESPIRATION MEASUREMENT
• NOWADAYS – CYBERKNIFE, SURGICAL ROBOT DA VINCI, ARTIFICIAL HEART AND MANY OTHER..
HOW IT’S LOOK
LOCALLY OR REMOTELY?

- LOCAL OR REMOTE TREATMENT?
- NO OBSTACLES FROM TECHNOLOGY TO COLLECT PATIENT DATA...
- ...HOWEVER SAME PROBLEMS HAVE TO BE ADRESSED (TO BE CONSIDERED LATER)
- LEGAL PROBLEM – SOME COUNTRY – MEDICAL TREATMENT ALLOWED ONLY IN PERSON!
- WHO IS RESPONSIBLE – DOCTOR IN REMOTE LOCATION, LOCAL STAFF OR SOMONE ELSE?
- LETS TRY TO NAME ISSUES...
ISSUES

- LEGAL
- SOCIOLOGICAL
- PSYCHOLOGICAL
- ETHICAL
- TECHNICAL
- SECURITY (MEDICAL AND TECHNICAL)
TYPE OF RELATION

- H2H
- H2M AND VICE VERA
- M2M2H
- AND MUCH MORE ...

Source: YouTube
IOT, REALLY?

- REMOTE PROCES (H2H, M2M, H2M) REQUIRED IDENTIFICATION
- WHO IS ON SECOND SIDE OF CHANNEL?
- SENSITIVE PROCESSES REQUIRED STRONG AUTHENTICATION
- SEVERAL ISSUES RELATED TO IDENTIFICATION ENTITY
- WHO IS RESPONSIBLE OF LEGAL POINT?
- HOW TO EVALUATE DIFFERENT METHODS?
- WHO SHOULD DO IT?
AUTHENTICATION - SET OF ISO/IEC STANDARD

• ISO/IEC 9798-1:2010 PART 1: ENTITY AUTHENTICATION –PART 1: GENERAL
• ISO/IEC 9798-2:2008 PART 2: MECHANISMS USING SYMMETRIC ENCIPHERMENT ALGORITHMS
• ISO/IEC 9798-3: 1998 PART 3: MECHANISMS USING DIGITAL SIGNATURE TECHNIQUES
• ISO/IEC 9798-4: 1999 PART 4: MECHANISMS USING A CRYPTOGRAPHIC CHECK FUNCTION
• ISO/IEC 9798-5: 2009 PART 5: MECHANISMS USING A CRYPTOGRAPHIC CHECK FUNCTION
• ISO/IEC 9798-6: 2010 PART 6: PART 6: MECHANISMS USING MANUAL DATA TRANSFER

• ISO/IEC 9797 MESSAGE AUTHENTICATION CODES (MACS)
  • — PART 1: MECHANISMS USING A BLOCK CIPHER
  • — PART 2: MECHANISMS USING A DEDICATED HASH-FUNCTION
  • — PART 3: MECHANISMS USING A UNIVERSAL HASH-FUNCTION

• ISO/IEC 29115: 2013 ENTITY AUTHENTICATION ASSURANCE FRAMEWORK

IEEE IoT WORKSHOP 2017-07-25 PRAHA
WHAT NEXT - ISO/IEC JTC1/SC27/WG5

Biometrics - The use of biometric technology in commercial Identity Management applications [29144; SC37]

Authentication Context for Biometrics (24761:2009/Cor 1:2013)

Biometric Information Protection (24745:2011)

Biometrics - Jurisdictional and societal considerations for commercial applications - Part 1: General Guidance (TR 24714:2008; SC37)


Biometrics - Presentation Attack Detection (30107; SC37)

Telebiometric authentication framework using biometric hardware security module (ITU-T X. 1085 (bsm) | ISMEC 17922)

Source: Państwowy Instytut Łączności

IEEE IoT WORKSHOP 2017-07-25 PRAHA
ISO/IEC 29115

- LEVEL OF ASSURANCE (FROM 1 TO 4)
- ACTORS (WHO IS INVOLVED)
- ENTITY AUTHENTICATION ASSURANCE FRAMEWORK PHASES
  - ENROLMENT PHASE
  - CREDENTIAL MANAGEMENT PHASE
  - ENTITY AUTHENTICATION PHASE
- MANAGEMENT AND ORGANIZATIONAL CONSIDERATION
- THREATS AND CONTROLS
- SERVICE ASSURANCE CRITERIA
# REQUIRED LEVEL OF ASSURANCE

<table>
<thead>
<tr>
<th>LEVEL</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-low</td>
<td>Little or no confidence in the asserted identity</td>
</tr>
<tr>
<td>2- medium</td>
<td>Some confidence in the asserted identity</td>
</tr>
<tr>
<td>3-high</td>
<td>High confidence in the asserted identity</td>
</tr>
<tr>
<td>4-very high</td>
<td>Very high confidence in the asserted identity</td>
</tr>
</tbody>
</table>
HOW TO APPLY STANDARD IN MEDICAL WORD

• MEDICAL STAFF EQUIPED WITH CRYPTOGRAFIC CARD (CONTACT OR CONTACTLESS)
• CARD BASED ON COMMON CRITERIA CERTIFICATION (ISO/IEC 15 408) AT MINIMUM 4+LEVEL
• PROOF OF IDENTITY TROUGH USE OF IDENTITY INFORMATION FROM MULTIPLE AUTHORTATIVE SOURCES
• EXAMPLE - DOCTOR OR NURSES CHAMBER + DATA BASE OF AUTHORITY WHO ISSUED ID CARD
• BIOMETRIC- NOT NECESSERLY BUT HIGHLY RECOMMENDED
HOW TO APPLY STANDARD IN TECHNICAL WORD

• ONLY STRONG CRYPTOGRAFIC PROTOCOL MUST BE APPLY
• RESONABLE LENGTH OF CRYPTOGRAFIC KEY
• RISK ASSESMENT – DO IT PERMANENTLY!
• REMOVE NOT ENOUGH SECURE PROTOCOL IMMEDIATELY
• EXAMPLE- SSL V.3, MD5, SHA-1
• COMMUNICATION MUST BE ENCIFERED BY STRONG AND APPROVED ALGHORITM!
• AVOID OWN „BETTER AND CHIPPER” SOLUTION
• USE ONLY CERTIFIED SOLUTION – SOMETIME IT IS REQUIRD BY LOW

IEEE IoT WORKSHOP 2017-07-25 PRAHA
SUMMARY

• ENORMOUS TECHNICAL PROGRESS
• NEW CHANCE FOR PATIENT
• SOPHISTICATED TECHNOLOGY AND PROTOCOLS
• SECURITY ISSUES
• STANDARISATION
• LEGAL REQUIREMENT

• LAST BUT NOT LEAST – PATIENT IS NOT A THINGS!