Securing the E-Health Cloud

Hans Löhr
Horst Görtz Institute
for IT Security
Ruhr-University Bochum
Germany
hans.loehr@trust.rub.de

Ahmad-Reza Sadeghi
Horst Görtz Institute
for IT Security
Ruhr-University Bochum
Germany
ahmad.sadeghi@trust.rustegity

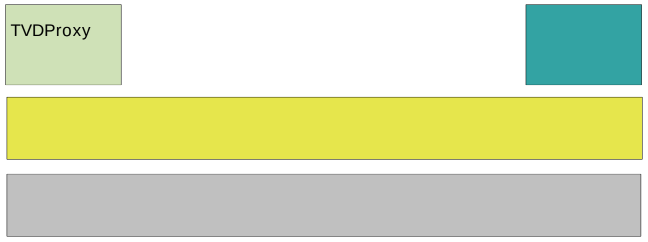
systems must accommodate various workflows, not only related to the patients' medical data, but also accounting and billing of treatments, medication, etc. Moreover, for

Figure 1: Simple E-Health Cloud model. Patients manage their own personal health records.

Figure 2: Advanced E-Health Cloud model. Health61fé1seoasd aoeeeteeo oe.]TJ0g0G1F58711.9552Tf7-18.7.51-29.63519Td[3(1000P F

means no other party is allowed to circumvent privacy decisions and access rights definitions of the patient regarding EHR data. But if the card issuer or even the EHR server providers maintain backup copies of the cryptographic keys for reasons of issuing backupmeea110.461 Td [(c)d523(rea)1(so8p335(t)1(n)1-363(o)(of)-335(ftk)1(u)o(erv)28(e)1(r)]TJ 0 -10.loso8p335s,)-5 dedicated healthcare network[4], and another system to store and process patients' medical data. In addition, the doctor needs web access and must be able to send and receive e-mails.

These different workflows should be separated from each other: The health insurance should not get access to the detailed medical data, and security problems arising from In-


TVDProxy

any time. This requires the introduction of a storage management infrastructure in order to handle, e.g.,