# Integrity and non-repudiation of VoIP streams with TPM2.0 over Wi-Fi networks

K.-O. Detken · M. Jahnke · M. Humann (DECOIT GmbH)
B. Röllgen (Global IP Telecommunications Ltd.)


Prof. Dr. Kai-Oliver Detken
DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen
https://www.decoit.de
detken@decoit.de


© DECOIT GmbH

# Agenda

- Motivation
- VoIP security
- INTEGER project
- Scenario examples
- TPM implementation
- Data format (Clearmode and CBOR)
- Conclusions


© DECOIT GmbH

# Motivation

- Digitalization of telecommunications networks and the Internet platform itself allows new attack scenarios
- Voice over IP (VoIP) communication can be established between random nodes – therefore eavesdropping can be happened everywhere
- Encryption is not the only solution to compensate attacks, because of in many cases you have to know which participants called each other
- Secure authentication and integrity of VoIP communication is the recommendation

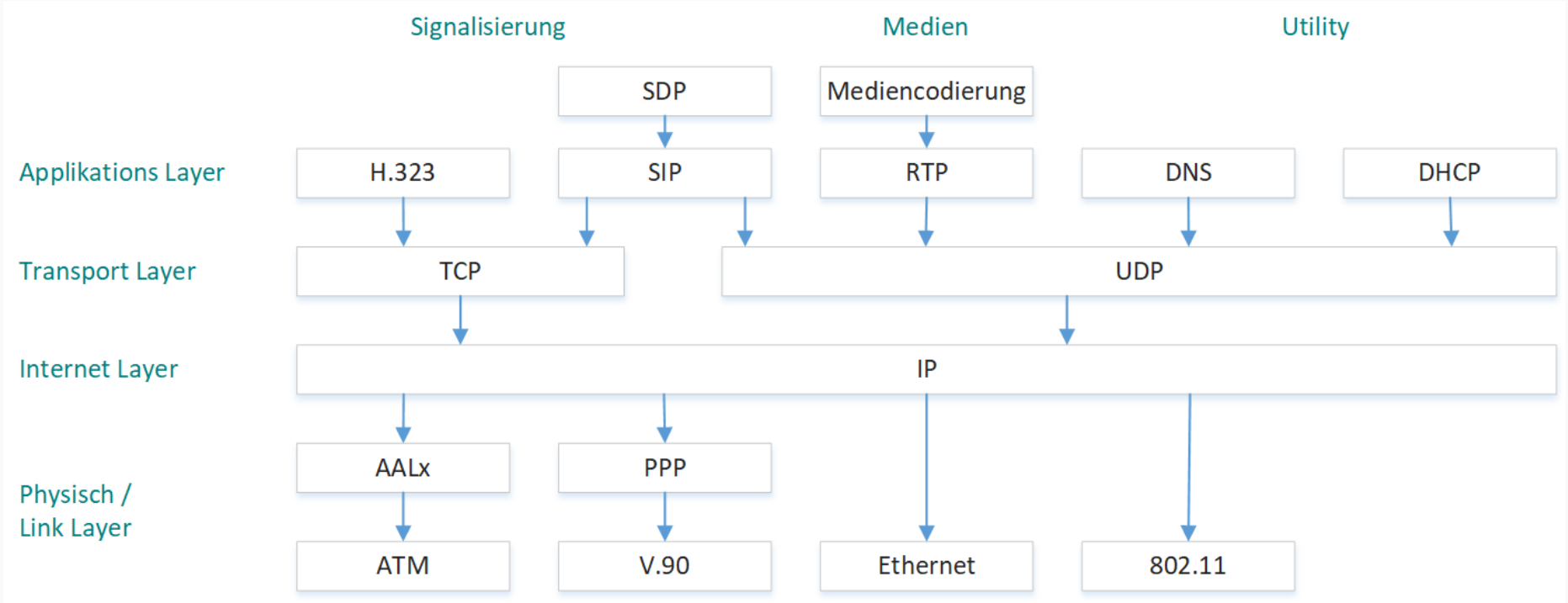

© DECOIT GmbH

# VoIP security

- VoIP will not be limited to cable networks: Convergent speech and data transmission will affect next generation mobile networks and Wi-Fi networks as well
- Efforts to add security features to VoIP products are currently infrequently deployed, though proposals for privacy protection exist (like SRTP for end-to-end encryption)
- In fact, the most providers don't offer VoIP security features to their customers
- While the problem of eavesdropping is solved for digital networks (at least in theory), hardly any effort to add non-repudiation is made


© DECOIT GmbH

# VoIP protocols





© DECOIT GmbH

# INTEGER project

- INTEGER = Integrity and non-Repudiation of multimedia VoIP streams
- INTEGER is a cooperation project within the German BMWi (ZIM) with the following partners:
  - DECOIT® GmbH (coordinator and developer)
  - University of Applied Sciences of Bremen (research)
  - Global IP Telecommunications Ltd. (softphone vendor, devoloper)
  - reventix GmbH (VoIP provider)
- Associated partner:
  - Infineon AG (German vendor for TPM-Chips)
  - Fraunhofer SIT (German institute with VoIP patent and expertise)
- The project has been started at July 2017 and will end at June 2019
- Project website: http://www.integer-project.de


© DECOIT GmbH

# Focus of INTEGER

- *Protection of the integrity of voice conversations*: Protecting a (recorded, digital) voice conversation from falsification and tampering differs from protecting the integrity of other digital data due to the relevance of the temporal context.
- *Authentication of speakers*: Initial authentication of callers in conjunction with inherent biometric authenticity of voice is the basic approach to this problem. It has to be noted that each authentication of a speaker requires trust in the devices used by the communicating parties.
- *Digital signatures over voice conversations*: Building on the first two tasks it is possible to achieve, for voice conversations, the level of non-repudiation provided by digital signatures over digital documents, e.g. an expression of will. For this, the aforementioned tasks must be complemented by a proof of possession of a trustworthy signature token and device, and the intention to sign.


© DECOIT GmbH

# Main goals of INTEGER

- INTEGER has the goal to protect the integrity of a communication between two parties
- Additionally INTEGER wants to secure authentication of both parties by an electronical signature and/or a hardware trust anchor
- A public key infrastructure (PKI) is not foreseen for this scenarios
- An secured archive of the communication data is necessary to achieve this

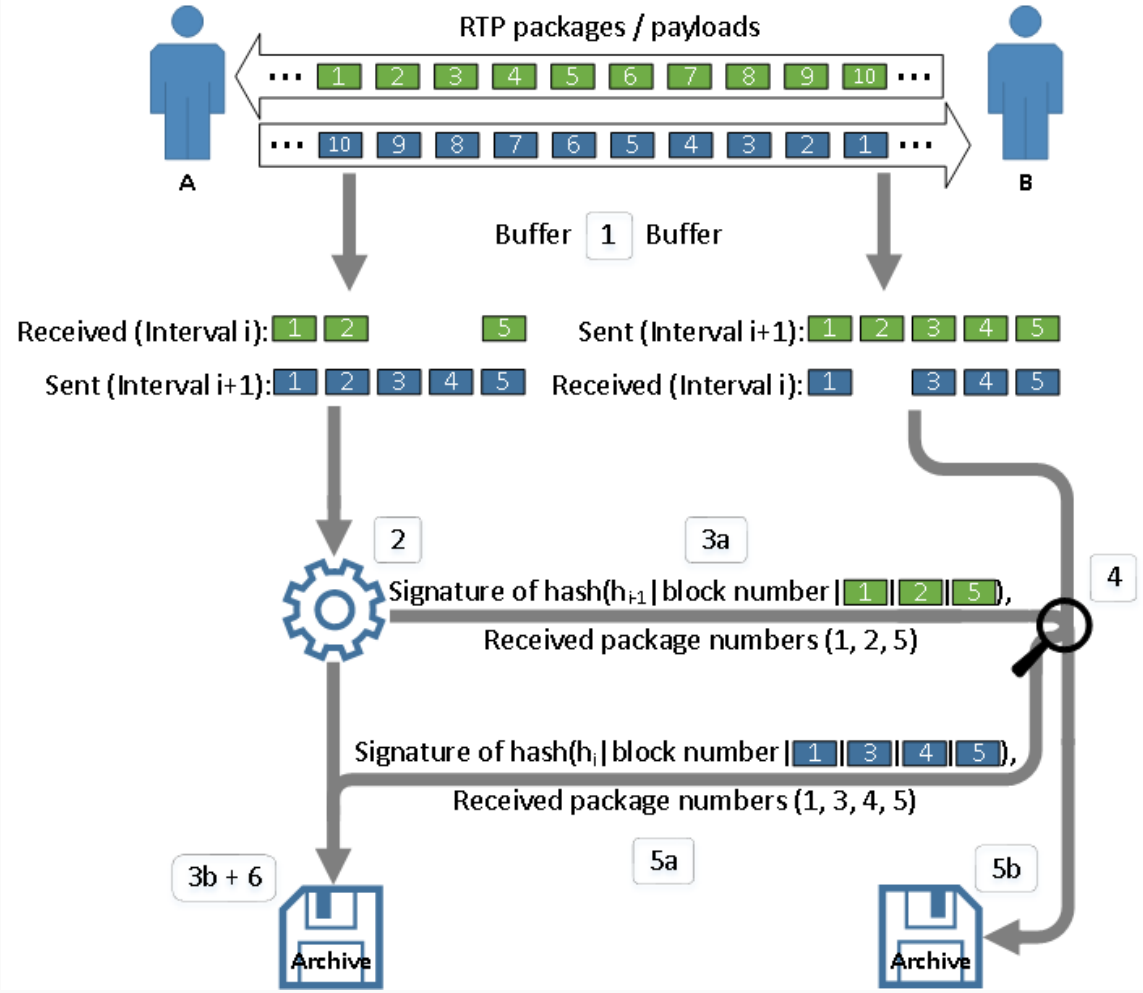

© DECOIT GmbH

# Scenario example

- Two business partners agree an a contract during a VoIP conversation
- The contract should be finalised during the communication to save time
- Both parties use a compatible end-device, which can be used to type in a PIN number
- Afterwards both parties marked the conversation for archiving it
- This signalling process of an archiving will be closed if the communication ends


© DECOIT GmbH

# Flow diagram of communication





© DECOIT GmbH

# Proposed concept

- The core concept ensures
  - integrity,
  - cohesion, and
  - non-repudiation of a conversation
- This can be reached by creating a signed hash chain covering all individual RTP-packets exchanged between the two communication parties
- It works by
  - buffer of all communication data
  - signatures over current hash sums and cross checks
  - signatures of the archive

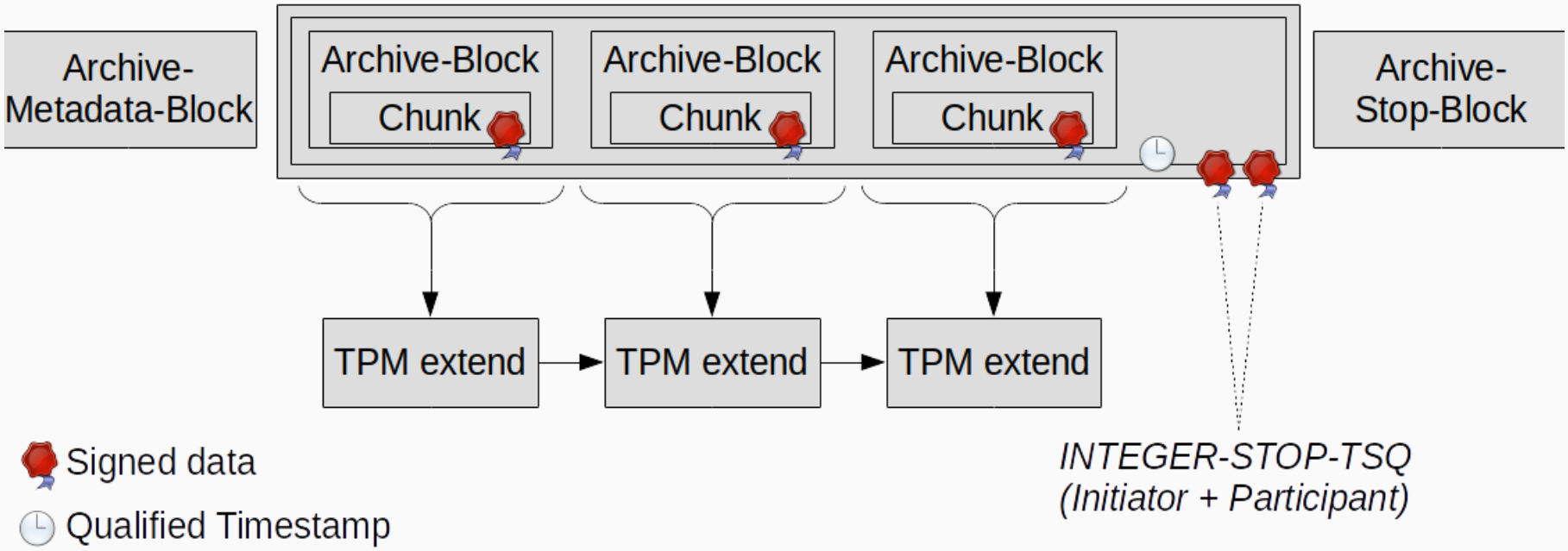

© DECOIT GmbH

# TPM integration


- Trusted Platform Module (TPM) has been used as a hardware-based trust anchor
- Especially that is necessary in insecure environments like Wi-Fi communications
- TPM chips are able to create, store, and handle keys for users in a secure way
- A TPM chip can help determining that the used hardware or software has not been manipulated
- For this purpose, the TPM collects the required information and stores it as hash values in the so-called Platform Configuration Registers (PCR)
- These values can be exported as a TPM-Quote that is signed by the TPM: a comparison of external/internal values is possible


© DECOIT GmbH

# Archiving with TPM





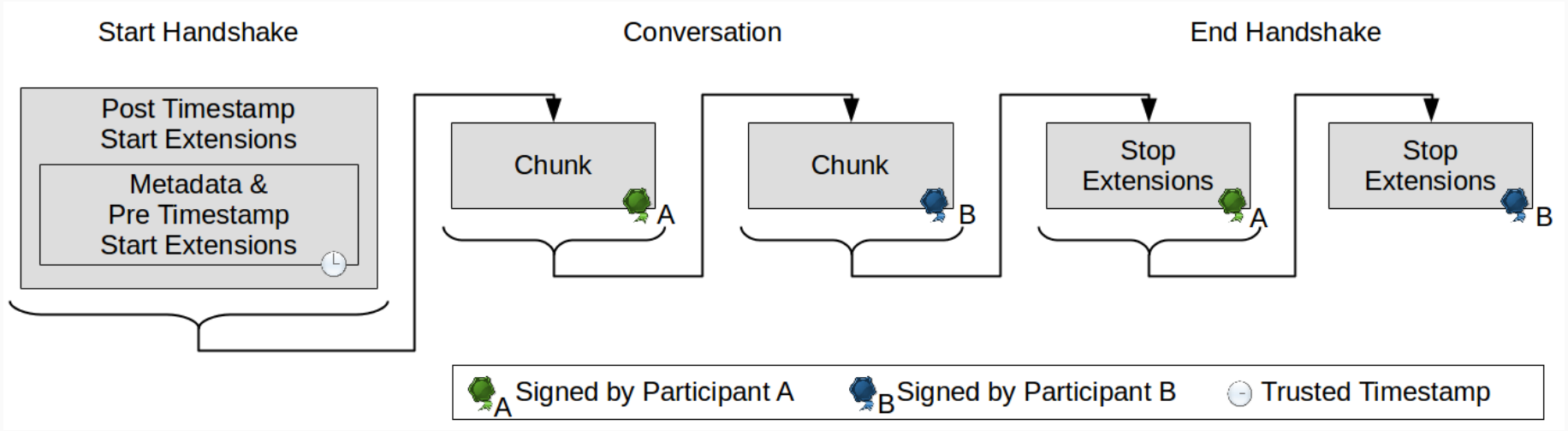
© DECOIT GmbH

# TPM implementation


- INTEGER uses the TPM 2.0 specification
  - Algorithms SHA-256, SHA-512
  - Elliptic curves
- Main use of TPM within the project:
  - Secure storage of hash values, which have build via a data structure
  - Ensure that hard- and software have not been manipulated
- Implementation
  - Verification of manipulation via hash chain
  - Asynchronous access to TPM chip, because of performance delay
  - Sequence is guaranteed by exchange of stop signals


© DECOIT GmbH

# Hash chain without TPM





© DECOIT GmbH

# Hash chain without TPM

- Both parties exchange their certificates used in the signing process
- The certificate of the party initiating the session has to be a qualified certificate
- The second party is allowed to use a self-signed certificate (business to consumer scenario)
- The end-handshake allows the protocol to properly finish a signing session
- The actual hash value is not transmitted, only the information needed to calculate it
- That scenario has not TPM support regarding performance issues


© DECOIT GmbH

# Data format

- Both parties require the same data representation of RTP payloads to be able to update the hash chain and verify the signature of the other party
- VoIP carrier gateways, however, usually are allowed to convert this data between various codecs, preventing the participants from verifying each other's signatures
- As this problem also affects other protocols, such as ISDN, the Clearmode (RFC 4040) pseudo-codec was introduced
- In Clearmode audio packets can be transmitted as well as additional protocol data in the same RTP stream
- Clearmode uses no encoding or decoding!


© DECOIT GmbH

# CBOR (RFC 7049)

- To reduce the size of the packets sent to the archive, especially in a wireless environment, the Concise Binary Object Representation (CBOR) is used in the prototypical implementation, with the option to switch to a more sophisticated design if necessary
- CBOR is based on a JSON data model and is encoded in binary: this saves bandwidth and allows for faster processing
- One of the main goals for the development of CBOR was the Internet of Things (IoT), which includes very simple, inexpensive nodes
- Therefore, CBOR is also very useful in wireless low-bandwidth environments


© DECOIT GmbH

# Conclusions

- Main goal of INTEGER is providing integrity and non-repudiation of internet-based multimedia communication of VoIP
- Currently there are no solutions like INTEGER for B2B or B2C on the market
- Use scenarios are:
  - Protection of integrity in a point-to-point communication scenario
  - Secure authentication of both communication parties
- By the use of digital signatures and TPM chips the optimal result can be reached
- The softphone of Global IP Telecommunications will be extended with this INTEGER feature
- The provider reventix will use the softphone of INTEGER in their network for customers


© DECOIT GmbH

# Thank you for your attention!

**DECOIT GmbH**
Fahrenheitstraße 9
D-28359 Bremen

https://www.decoit.de
info@decoit.de




© DECOIT GmbH