Integrität und Nicht-Abstreitbarkeit von VoIP-Kommunikation

K.-O. Detken, M. Jahnke (DECOIT GmbH)

B. Röllgen (Global IP Telecommunications Ltd.)

DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen
https://www.decoit.de
info@decoit.de

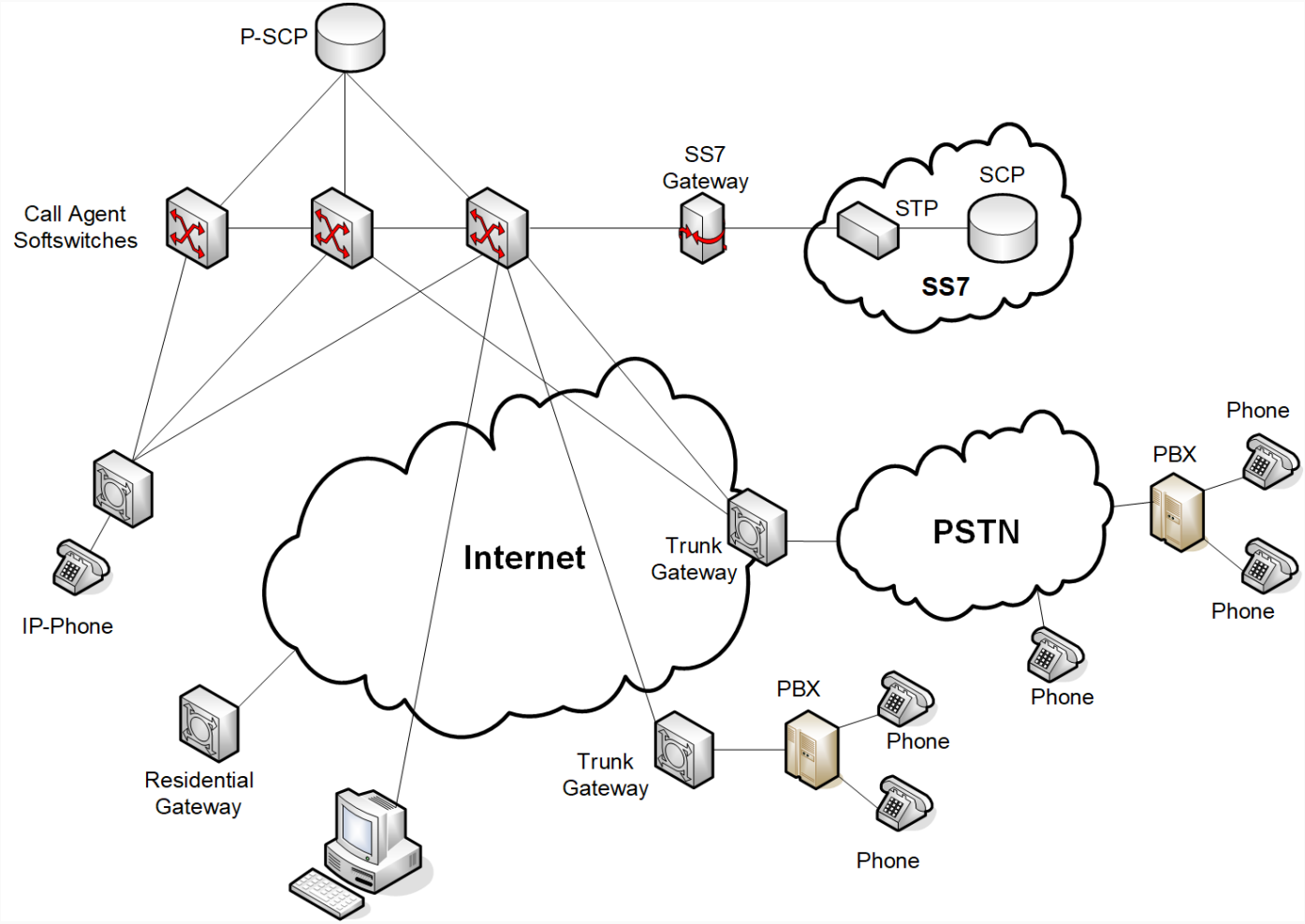
Agenda

- Einleitung
  - VoIP-Szenarien und -Protokollstapel
  - Kooperationsprojekt
  - Motivation
  - Ziele
- Umsetzung
  - Beispielszenario
  - Kommunikationsablauf
  - TPM-Integration
  - Clearmode
- Fazit

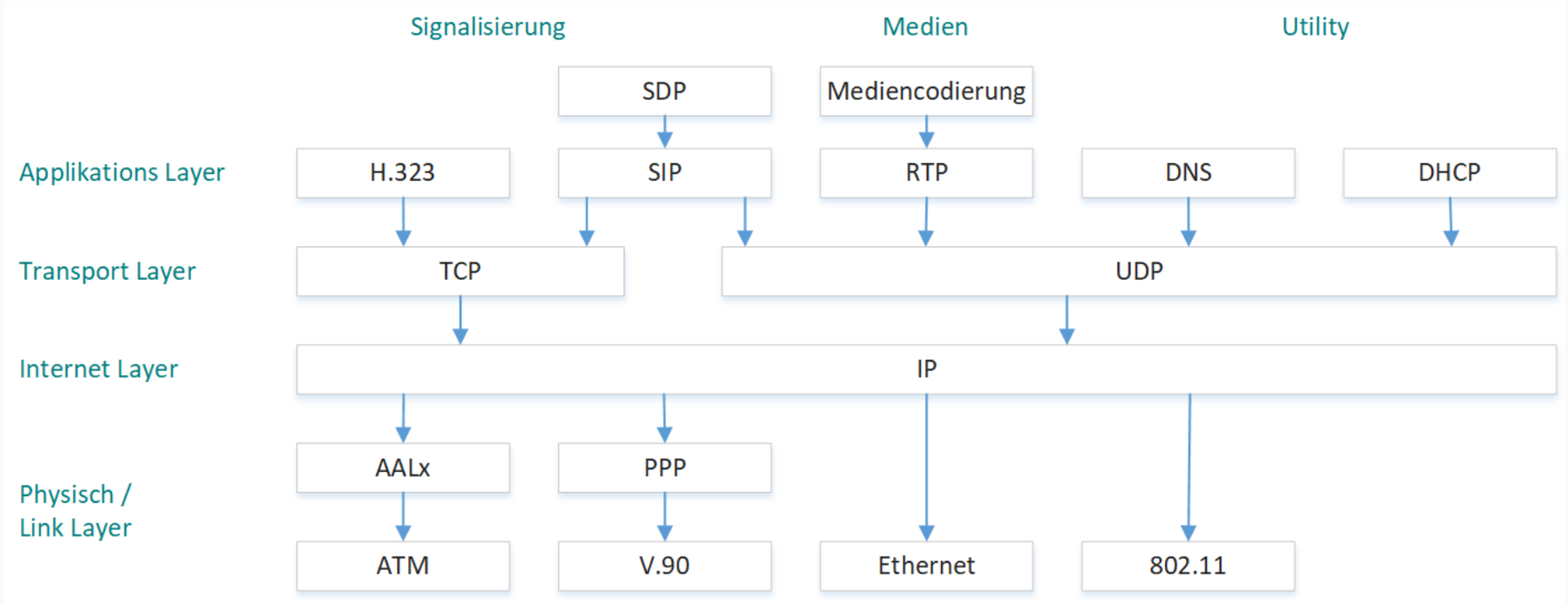
Einleitung
VoIP-Szenarien (1)

- **Campus VoIP:** In einer Campus-VoIP-Umgebung wird eine Nebenstellenanlage auf IP-Basis verwendet, die auch als IP-PBX (Private Branch eXchange) bezeichnet wird.
- **IP Centrex/Hosted IP:** Diese VoIP-Variante beinhaltet eine virtuelle IP-basierte Nebenstellenanlage, die von einem Provider zur Verfügung gestellt wird.
- **VoIP-Trunks:** Dieses Szenario beinhaltet direkte Punkt-zu-Punkt-Verbindungen zwischen verschiedenen Standorten.

Einleitung
VoIP-Szenarien (2)



Einleitung
VoIP-Protokollstapel



Einleitung
Kooperationsprojekt

- 2-Jahres-Projekt ZIM (BMWi)
- Zeitdauer 01.07.2017 – 30.06.2019
- URL-Adresse: www.integer-project.de
- Projektziel: Integrität und Nicht-Abstreitbarkeit der internetbasierten multimedialen Kommunikation
- Partner:
  - Industrie: DECOIT® GmbH, Global IP Telecommunications Ltd., reventix GmbH
  - Hochschulen: Hochschule Bremen

Einleitung
Motivation

- Vollständige Digitalisierung der Nachrichtentechnik
  - Abhören ohne physikalischen Zugang
  - Unbegrenzte Zahl an Knoten zwischen den Endgeräten
  - Verschlüsselung der Verbindung reicht nicht aus
  - Identifizierung der Personen nicht sicher
- Sprache ist synthetisierbar
- Paradigma ist IP-basierte Telefonie
- Beweis für mündliche Vertragsabschlüsse ist teilweise schon Pflicht

Einleitung
Ziele

„INTEGER hat das Ziel den Schutz der Integrität einer Kommunikation und die sichere Authentifizierung der Kommunikationspartner, durch das elektronische Signieren der Kommunikation, zum Ziel gesetzt.“

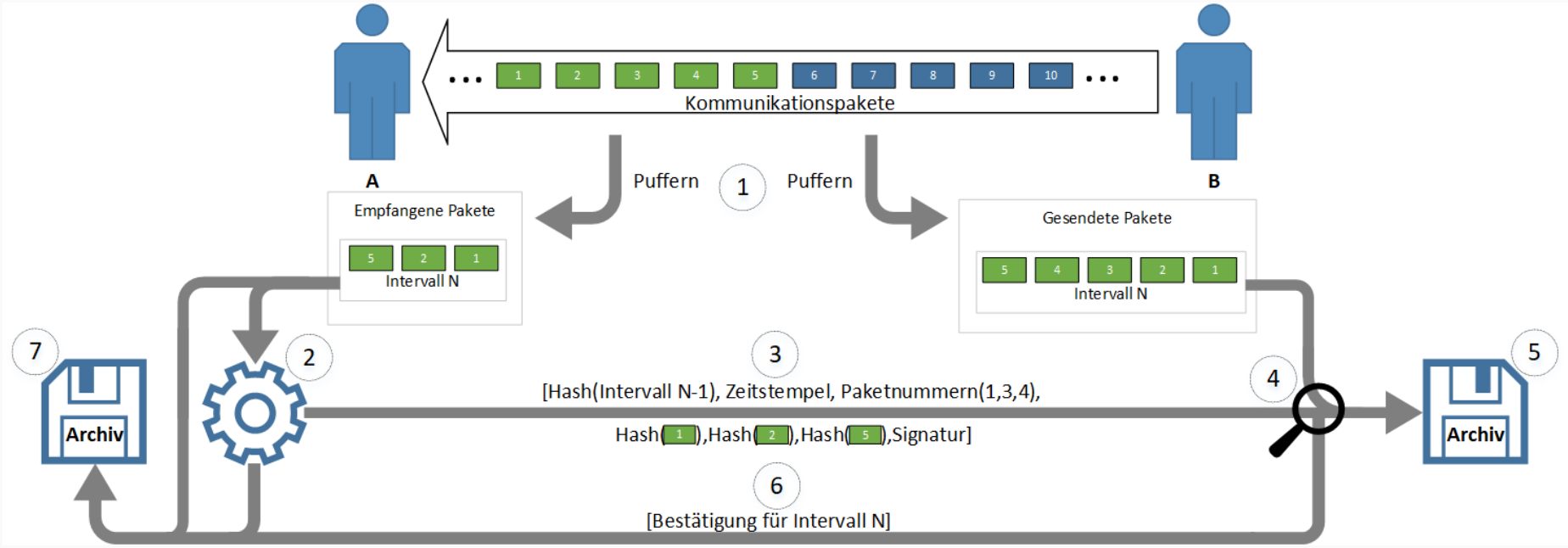
Einleitung
Ziele

- Integritätsschutz der Konversation
- Authentifizierung der Kommunikationspartner
  - Elektronische Signierung
  - Mit Hardware-Vertrauensanker
- Für B2B und B2C
- Ohne aufwendige Public-Key-Infrastruktur
- Revisionssichere Speicherung der Kommunikation

Umsetzung
Beispielszenario

- Zwei Geschäftspartner einigen sich auf Bedingungen und Konditionen eines Vertrages per VoIP-Verbindung
- Der Vertrag soll über das VoIP geschlossen werden, um Zeit zu sparen
- Beide Parteien haben ein kompatibles Endgeräte, das z.B. eine PIN-Eingabe erfordert
- Danach wird beiden Seiten signalisiert, dass die Kommunikation nun aufgezeichnet wird
- Der Signierungsprozess wird am Ende des Gespräches explizit beendet oder abgebrochen, wenn der Hörer aufgelegt wird

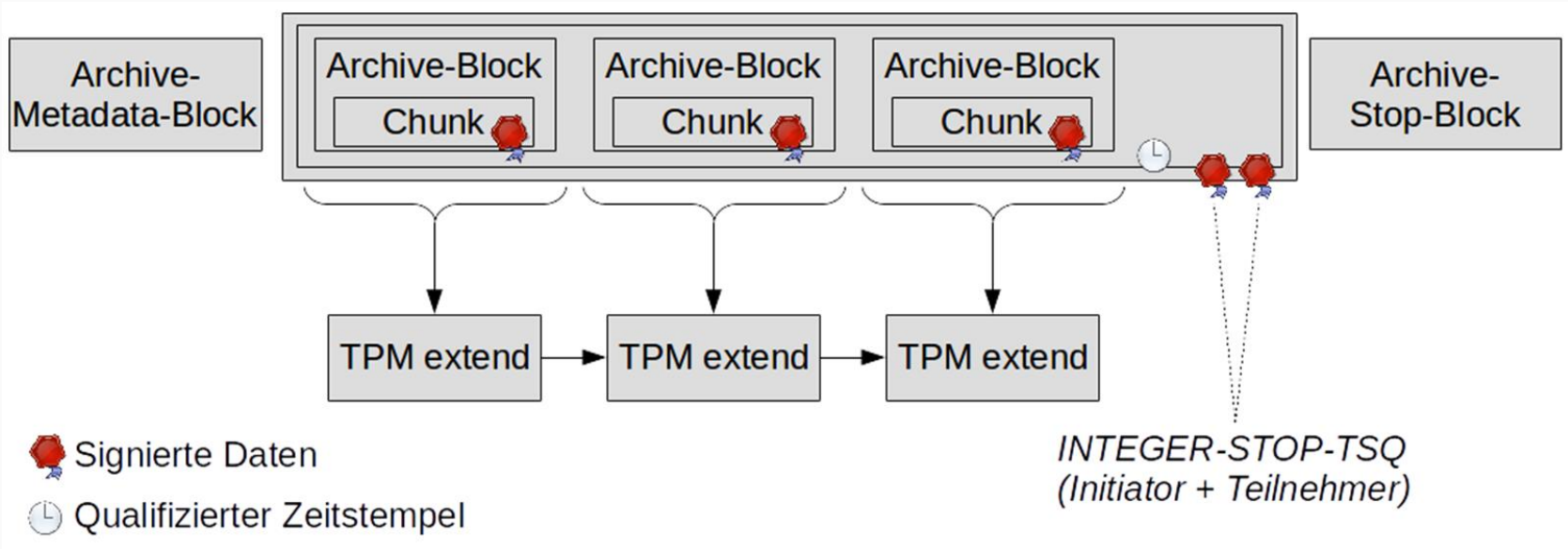
Umsetzung
Kommunikationsablauf



Umsetzung
TPM-Integration

- TPM dient als Hardware-Vertrauensanker
- Erzeugung, Speicherung und Benutzung von Schlüsseln
- Vor Gebrauch kann sichergestellt werden, dass Hard- und Software nicht manipuliert sind
- INTEGER nutzt die TPM2.0-Spezifikation
- Infineon hat keinen TPM-Chip nach CCEAL4+
  - Algorithmen SHA256, SHA512 und
  - Elliptische Kurven
- Sichere Speicherung von Hash-Werten, die über eine Datenstruktur gebildet wurden

Umsetzung
TPM-Integration



- Nachweis von Manipulation über Hash-Kette
- Diese wird parallel zur erfolgreichen Signierung
- Zugriff auf TPM nur asynchron, da Zugriffszeiten zu hoch
- Möglichkeit der Vertauschung von Paketen mit gleicher Blocknummer
- Tatsächliche Reihenfolge wird durch den Austausch des Stopp-Signales garantiert

Umsetzung
Clearmode

- Clearmode ermöglicht transparenten Transport von RTP-Daten nach RFC 4040
- Es können beliebige Informationen transportiert werden
- Die Deutsche Telekom nutzt dieses Protokoll z.B. zur Steuerung von ISDN-Anlagen über VoIP
- Clearmode ist ein Grundmerkmal von VoIP-Medien-Gateways
  - Keine Nutzung von Encoding und Decoding
  - Nur die Paketierung wird unterstützt

Umsetzung
Clearmode

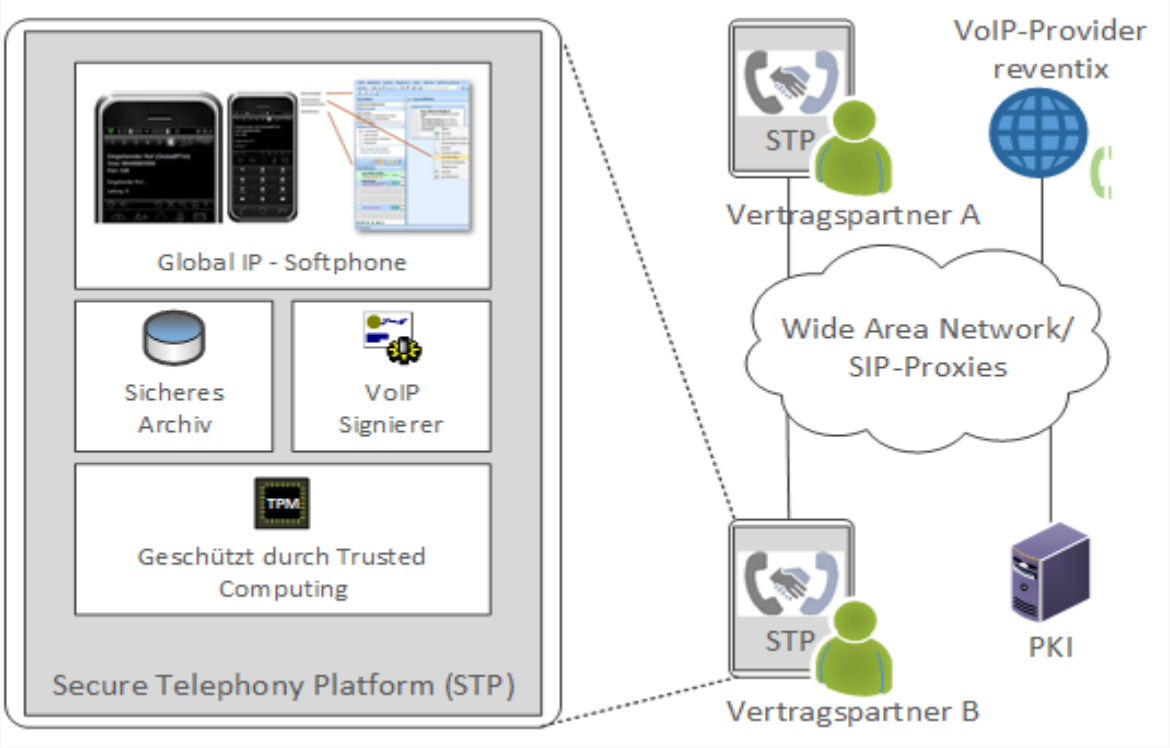
Aufbau eines Clearmode-Codecs:

Umsetzung
Clearmode

- Der Datenaustausch ist sampleorientiert
- Einschränkung in der Anzahl der Samples je Paket ist nicht vorhanden
- Nur IPv4-Pakete begrenzen auf 64 kByte
- In der Praxis wegen MTU auf ca. 1,5 Kilobyte pro Paket begrenzt
- Bietet die Möglichkeit unveränderbar Daten auszutauschen
- Als „Pseudo-Codec“ für INTEGER optimal
- Kombinierter Datenstrom von Integritäts-, Beweis- und VoIP-Daten

Anwendungsbereich

- Angestrebt ist eine völlig neuartige Form der Nicht-Abstreitbarkeit mündlicher Kommunikation
- Dies wird zum Teil bereits heute im Finanzsektor von der Europäischen Union gefordert
- Gerichtlich angeordnete Ausleitung von multimedialen Inhalten (TKÜ) ist ein weiterer Anwendungsfall



Fazit

- Ziel von INTEGER ist die Nicht-Abstreitbarkeit von multimedialer Kommunikation im VoIP-Bereich
- Im B2B- und auch B2C-Bereich fehlen aktuell solche Lösungen
- Anwendungsbereich ist:
  - Der Schutz der Integrität einer Kommunikation
  - Sichere Authentifizierung der Kommunikationspartner
- Dies soll mit Hilfe von elektronischen Signaturen und dem Einsatz des TPM-Chips hergestellt werden
- Realisierung mit dem Softphone von Global IP Telecommunications über den Provider reventix GmbH
- Aktuell befindet sich das INTEGER-Protokoll in der Implementierungsphase

Vielen Dank für Ihre Aufmerksamkeit!

DECOIT GmbH
Fahrenheitstraße 9
D-28359 Bremen

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