Security and Non-Repudiation for Voice-over-IP conversations

Abschlußvortrag Diplomarbeit

von Christian Hett (diplomarbeit-vortrag[at]c-hett.de)

Betreuer: Dr. Andreas U. Schmidt, Prof. Claudia Eckert

Fraunhofer Institut Sichere Informations-Technologie

Gliederung

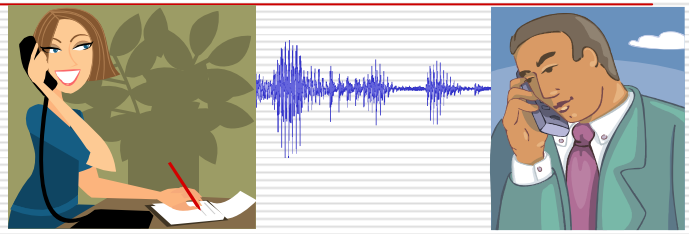
- Ziel und Ergebnis
- Vision und Use Case
- Überblick VoIP an Hand des SIP/RTP-Protokolls
- Signierszenario
- Konzept zum Signieren von Sprache
- Archivszenario
- Implementierung/ Demonstrator
- Screenshots
- Fragen und Diskussion

Ziel und Ergebnis

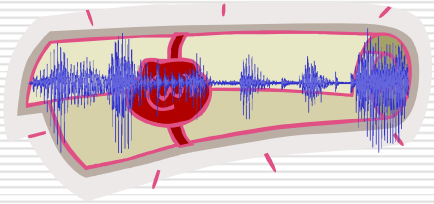
- Konzept und Protokolle wurden entwickelt, um für
  - natürlich sprachliche,
  - interaktive und
  - bidirektionale,

  per SIP/RTP geführte, paketbasierte Kommunikation
  - Nicht-Abstreitbarkeit zu gewährleisten,
  - die Integrität und zeitliche Abfolge zu schützen und
  - diese kontinuierlich zu signieren
- Dies erlaubt PKI-basierte, nicht-abstreitbare Signaturen über mündliche Abmachungen, Verträge und Angebote als Willenserklärung.
  ➔mündlicher Abschluß rechtlich bindender Verträge, ohne Bedarf an weiteren Zeugen und zwischen nicht persönlich bekannten Sprechern.
- Demonstrator wurde als Proxy-Server vor bestehenden SIP-Phones implementiert, um dieses Verfahren in einem selbst-signierten Archiv für VoIP-Kommunikation anzuwenden.

Vision und Use-Case (1/2)



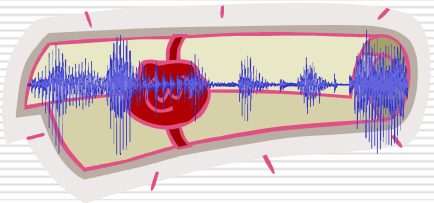
- Zwei Geschäftspartner verhandeln Bedingungen eines Vertrags über IP-Telefonie.
- Zu einem bestimmten Zeitpunkt entscheiden sie sich, den Vertrag mündlich abzuschließen, z.B. um Zeit und Ressourcen zu sparen
- Mit einem Authentifizierungstoken (Smartcard+ Pin oder Biometrie) initiieren sie den Signiervorgang
- Beide Parteien erfahren, dass der Anruf von diesem Moment an signiert und für die spätere Verwendung aufgezeichnet wird
- Sie legen den signierten Teil des Telefonats als Dokumentation des Vertrages in einem Archiv ab



Vision und Use-Case (2/2)

- Später bestreitet eine Partei Teile der Vereinbarung oder die Existenz des Vertrags.
- Die andere Partei bringt das signierte Telefonat als Beweisstück in den nun folgenden Gerichtsfall ein.
- Ein Gutachter bescheinigt
  - dass die digitale Signatur gültig ist
  - dass die Methode des Signierens sicher ist und dass der zeitliche Zusammenhang des Gesprächs erhalten wurde
- Ein weiterer Gutachter, der auf forensische Stimmenuntersuchung spezialisiert ist bescheinigt
  - die Identität der Sprecher
  - die phonetische Qualität und Verständlichkeit
  - dass das Gespräch nicht synthetisiert oder gefälscht ist

Das Gericht bestätigt die Gültigkeit des Vertrages. Erreicht wird ein

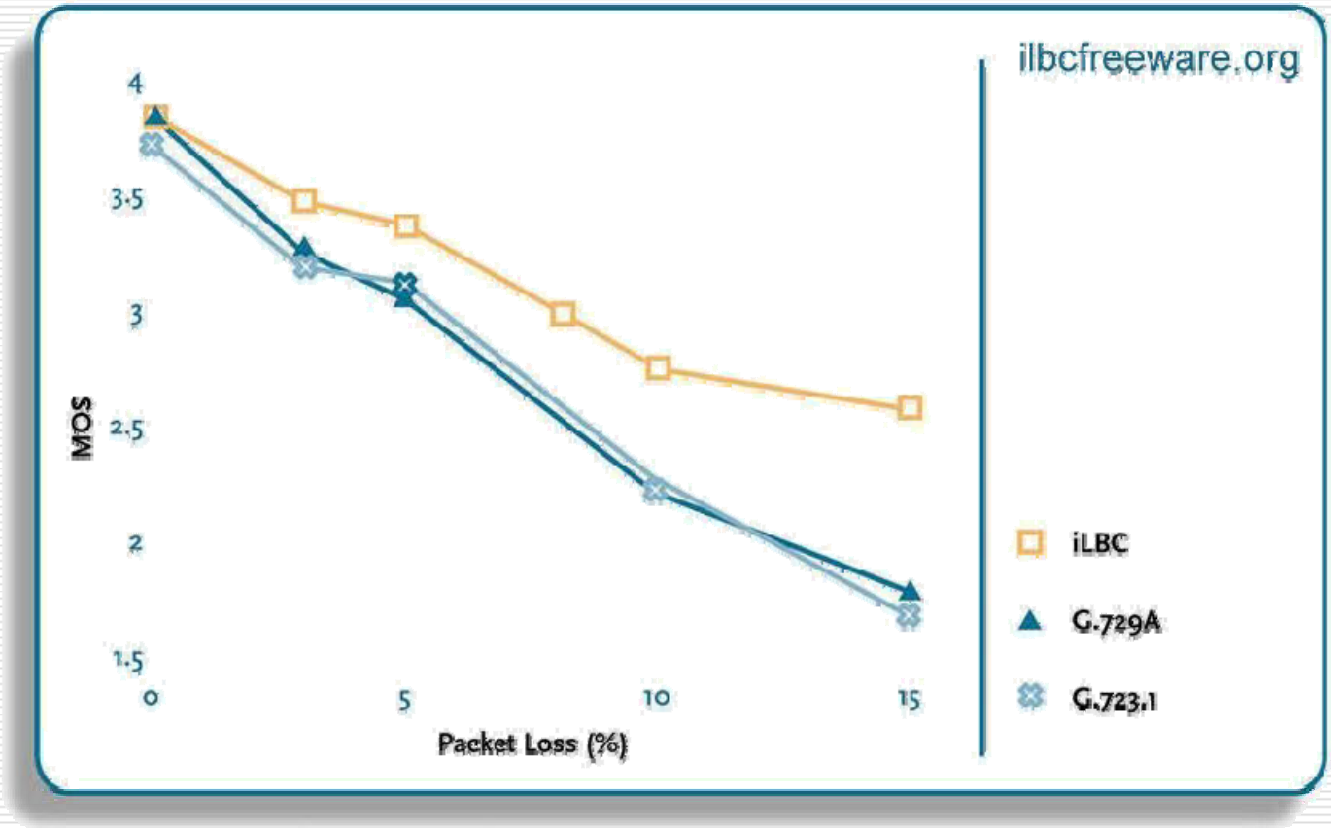


<u>Rechtlich bindender mündlicher Vertrag über VoIP ohne Zeugen</u>

Überblick Internettelefonie

- Massives Wachstum (Analysten: 20%-40% Wachstum…)
- Konvergenz der Netze
  - nur eine Leitung für Telefon und IP
  - bessere Ausnutzung der Bandbreite
- Paketvermittelt statt Leitungsvermittelt
- Codec (z.B. G.711, iLBC) komprimiert digitale Audiodaten
- Werden in kleine Pakete zerlegt, die ihren eigenen Weg im Netz suchen ➔ Schwankende Latenzzeit (Jitter), unterschiedliche Reihenfolge
- Keine Garantien für Ankunft/ Paketverlust ➔ Methoden zum Ausgleich des Paketverlusts je nach Codec
- Schutzziel Vertraulichkeit praktisch gelöst durch IPSEC oder SRTP

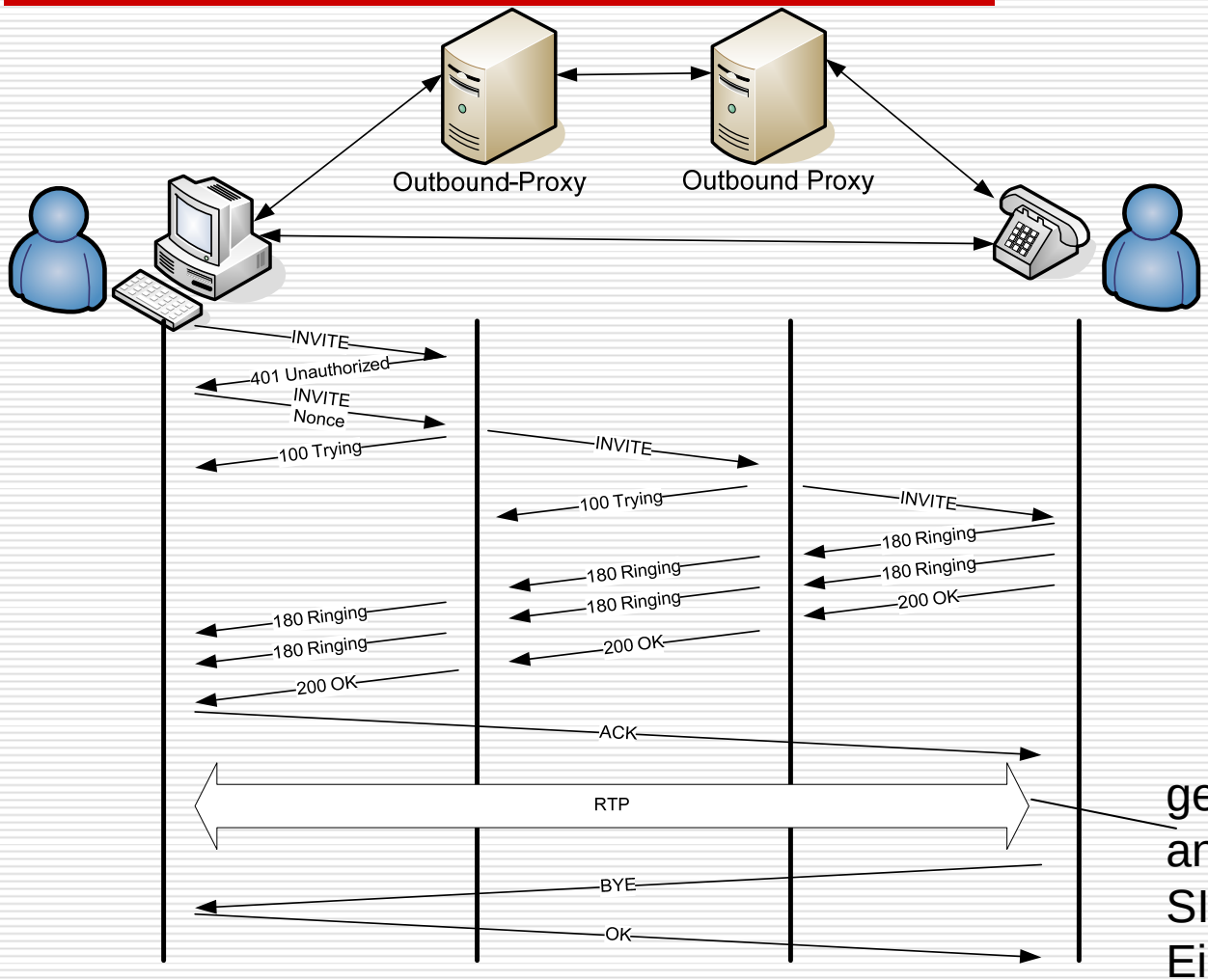
Sprachqualität / Paketverlust



The tests were performed by Dynstat, Inc., an independent test laboratory.
Score system range: 1 = bad, 2 = poor, 3 = fair, 4 = good, 5 = excellent

Außerdem: Paketlaufzeiten über 150ms führen zu Verlust der Illusion, gleichzeitig zu reden ➔ Kein Nachsenden der Pakete möglich, Signieren darf keine weitere Verzögerung bewirken

SIP - Session Initiation Protocol



getrennter Datenkanal,
andere Port-Nummern als
SIP-Signalisierung.
Ein RTP-Stream A→B
Ein RTP-Stream B→A

Beispiel: ankommender Anruf

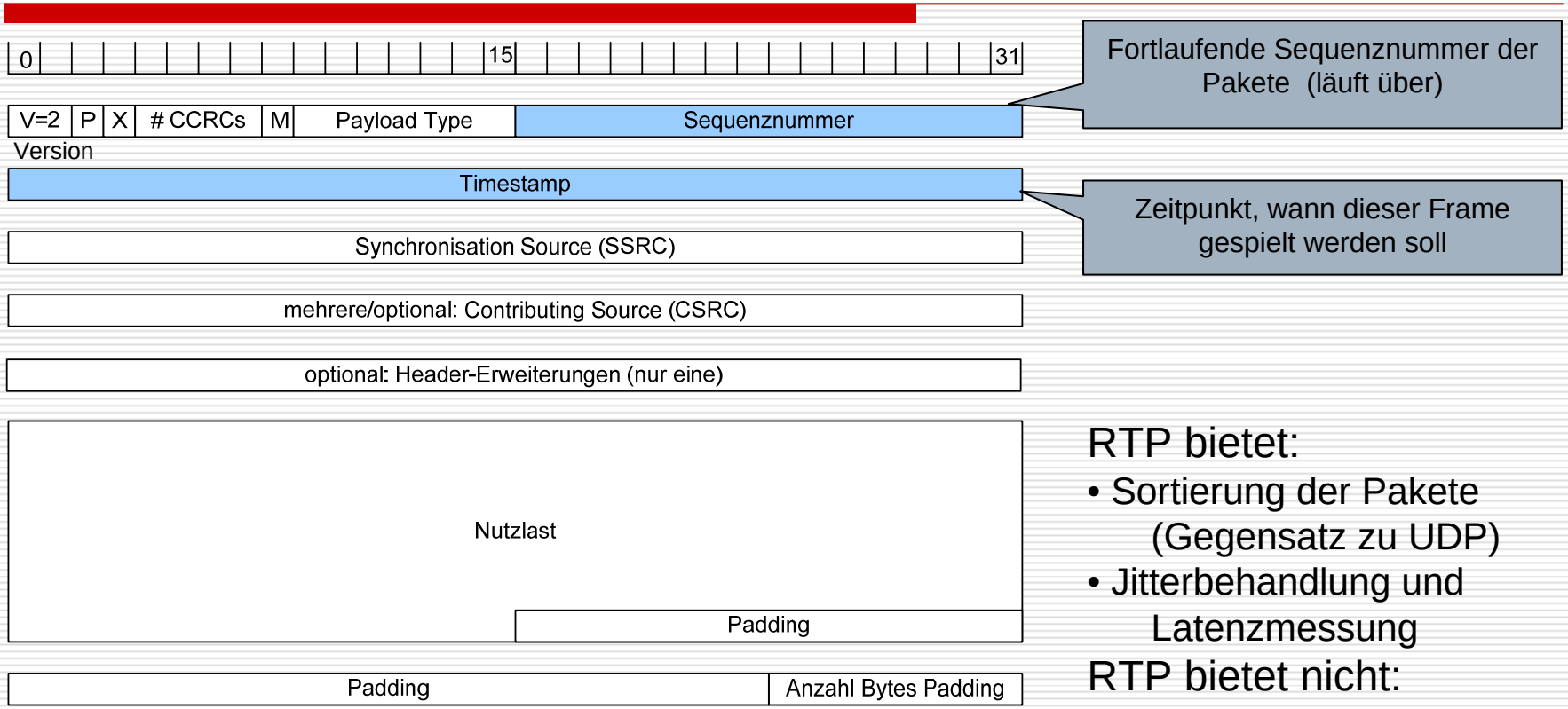
```
INVITE sip:49601234567@84.178.139.124:5070 SIP/2.0
Record-Route: <sip:212.227.15.225;ftag=1168841412;lr=on>
Record-Route: <sip:+49601234567@217.188.44.231;ftag=1168841412;lr=on>
Via: SIP/2.0/UDP 212.227.15.197;branch=z9hG4bK679d78391b60eeef2b991fb1c5eef30f
Via: SIP/2.0/UDP 212.227.15.225;branch=z9hG4bK8861.3b05c9c5.0
Via: SIP/2.0/UDP 212.227.15.197;branch=z9hG4bKca1305302a7d41c334b7e10607ff0942
Via: SIP/2.0/UDP 217.188.44.231;branch=z9hG4bK8861.ec83b004.0
Via: SIP/2.0/UDP 1und1-1.sip.mgc.voip.telefonica.de:5060 ;received=195.71.9.100;branch=z9hG4bKterm-1e5356-
      +491712345678-+49601234567
From: +491712345678 <sip:+491712345678@1und1-1.sip.mgc.voip.telefonica.de;user=phone>;tag=1168841412
To: +49601234567 <sip:+49601234567@1und1.interconnect.sip.voip.telefonica.de;user=phone>
Call-ID: 7dbde21a-6a92b0f7-73ae04b2-b982@subscriber1.interconnect.mgc.voip.telefonica.de
CSeq: 1 INVITE
Supported: timer
Session-Expires: 1800
Min-SE: 1800
Contact:  <sip:+491712345678@1und1-1.sip.mgc.voip.telefonica.de:5060>
Allow: INVITE,ACK,PRACK,SUBSCRIBE,BYE,CANCEL,NOTIFY,INFO,REFER,UPDATE
Max-Forwards: 6
Content-Type: application/sdp
Content-Length: 618
Diversion: <sip:49601234567@sip2.schlund.de;user=phone>;reason=additional

v=0
o=- 1710955 0 IN IP4 62.53.226.3
s=Cisco SDP 0
c=IN IP4 62.53.226.3
t=0 0
m=audio 18324 RTP/AVP 8 0 99 102 2 103 4 104 105 106 107 18 0 125 101 100
a=rtpmap:99 G726-16/8000
a=rtpmap:102 G726-24/8000
a=rtpmap:103 G7231-H/8000
a=rtpmap:104 G7231-L/8000
a=rtpmap:105 G729b/8000
a=rtpmap:106 G7231a-H/8000
a=rtpmap:107 G7231a-L/8000
a=rtpmap:125 GnX64/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=rtpmap:100 X-NSE/8000
a=fmtp:100 192-194,200-202
a=X-sqn:0
a=X-cap: 1 audio RTP/AVP 100
a=X-cpar: a=rtpmap:100 X-NSE/8000
a=X-cpar: a=fmtp:100 192-194,200-202
a=X-cap: 2 image udptl t38
```

SIP-Header

SDP-Body

RTP - Real-time Transport Protocol



- Overhead: ca. 12 Byte zu UDP-Paket dazu
- Payload Type:
  - 0-95: statisch
  - 96-127: dynamisch
  - per SDP ausgehandelt und definiert

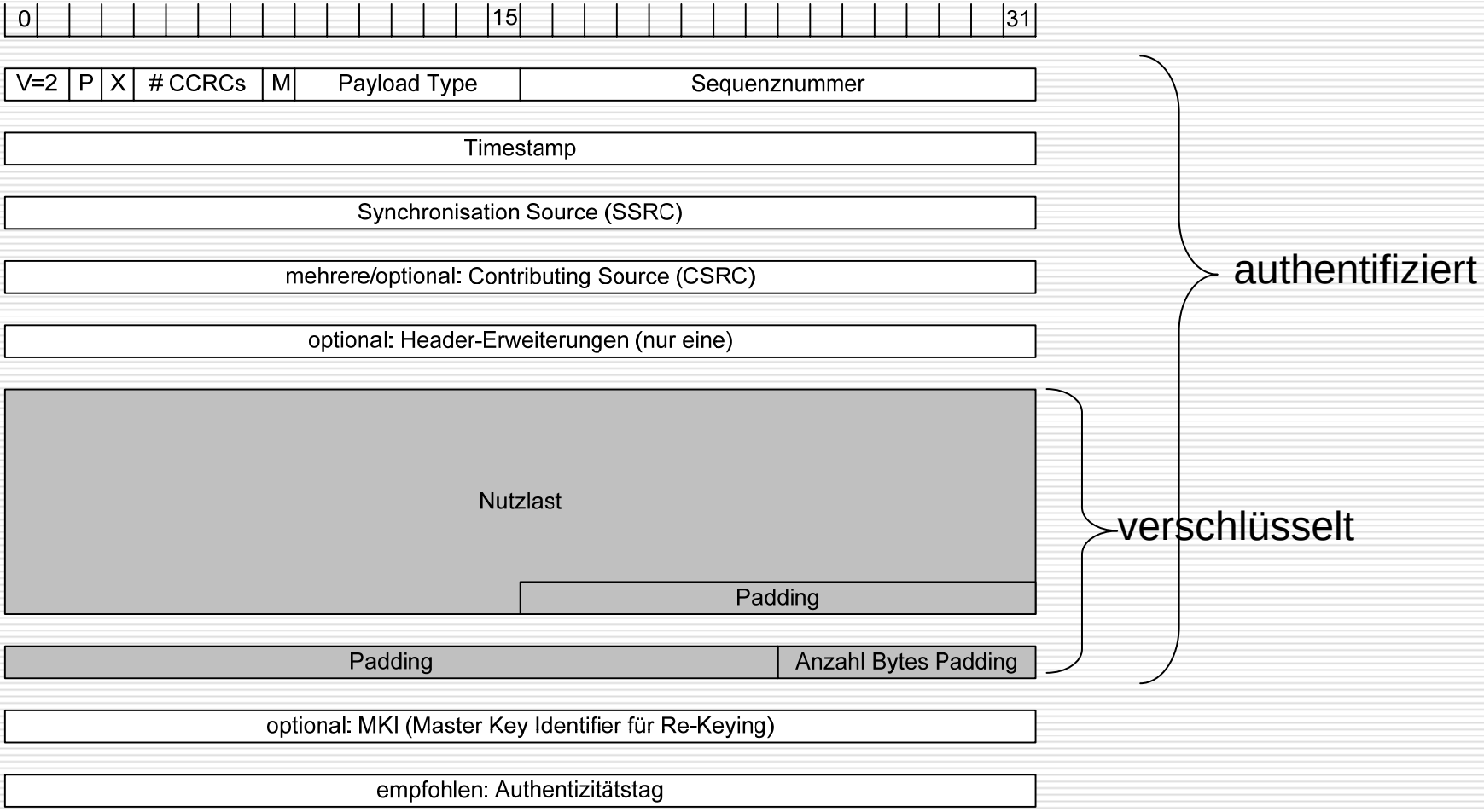
RTP bietet:

- Sortierung der Pakete (Gegensatz zu UDP)
- Jitterbehandlung und Latenzmessung

RTP bietet nicht:

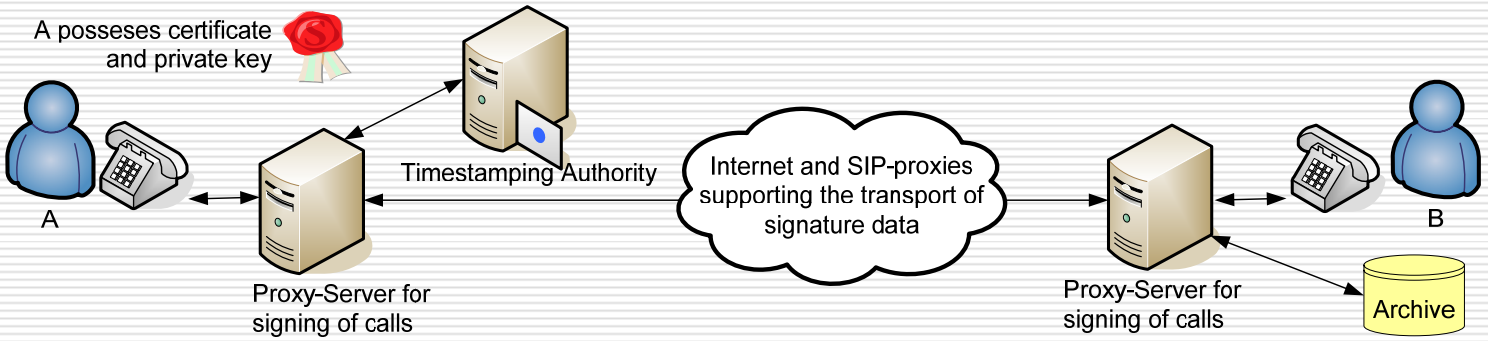
- Neuübertragung (Gegensatz zu TCP)

SRTP – Secure RTP



Vertraulichkeit, Authentizität (nur HMAC), Integrität: Prinzipiell gelöst, aber symmetrische Algorithmen

Signierszenario



- A besitzt privaten Schlüssel+ Zertifikat und möchte nicht-abstreitbare Willenserklärung (z.B. Angebot) abgeben.
- Signieren= explizite Zustimmung zur Aufzeichnung des Telefonats
- B zeichnet Gespräch auf (für Gericht/Gutachter)
- Zeitstempel bietet Anker für Schutz des zeitlichen Ablaufs/Kohäsion
- Interaktivität ermöglicht Rückfragen und Präzisierung und reduziert Präsentationsproblem ➔ A muß beide Kanäle der Kommunikation signieren, sonst fehlt Kontext

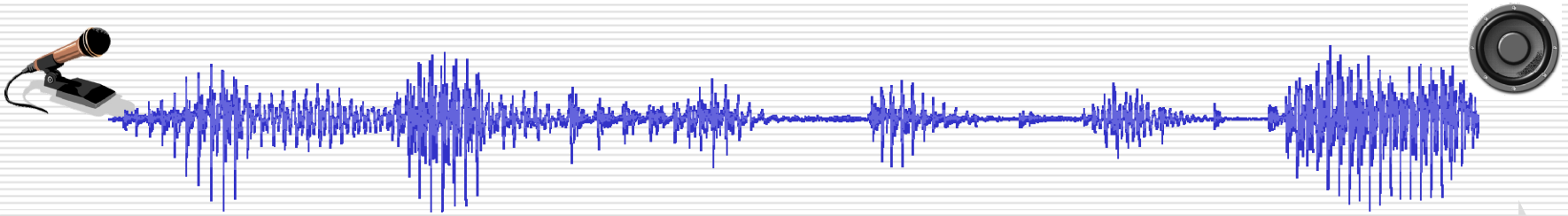
Was nicht gemacht wird...

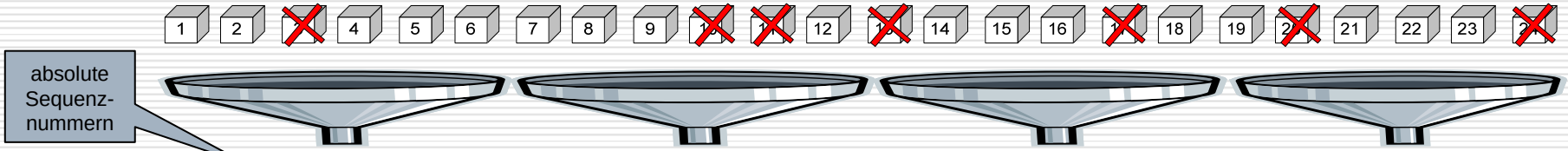
- WAV-Dateien aufnehmen, signieren und senden
  - Keine Interaktivität/ Duplexkanal, sondern Walkie-Talkie
  - Bereits jetzt per S/MIME E-Mail+ Windows Audiorekorder möglich ;-)
- **Jedes** RTP-Paket mit 1024 Bit RSA-Signatur versehen
  - Bei 44 Byte Nutzlast pro Paket zu großer Overhead (Speicherbedarf zu hoch)
  - Latenz erhöht sich zu stark (Skaliert nicht, zu hoher CPU-Aufwand auf mobilen Endgeräten)
  - Verkettung der Pakete nicht möglich, weil Ankunfsts-Reihenfolge varieren kann

Stattdessen Intervallbildung

- Ein Signieren des gesamten Gesprächs mit nur einer RSA-Signatur ist nicht möglich, da Gespräch jederzeit abbrechen kann
- Bis zur Trennung erfolgte Kommunikation ist bereits bindend. (→Aktien: “Kaufen!“)
- Kontinuierliches Signieren mit offenem Ende

  ➔ Intervalle bilden, alle Sprachpakete pro Intervall signieren, Signaturen verketten





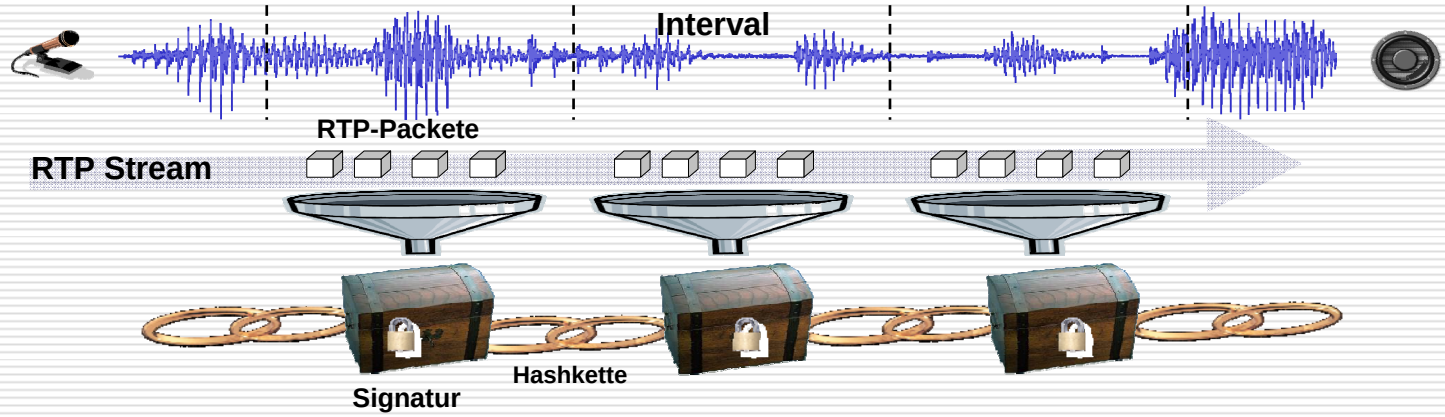
Packet-Lists	{1, 2, 4, 5, 6}	{7, 8, 9, 12}	{14, 15, 16, 18}	{19, 21, 22, 23}
Hashes:	{h(1), h(2), h(4), h(5), h(6)}	{h(7), h(8), h(9), h(12)}	{h(14), h(15), h(16), h(18)}	{h(19), h(21), h(22), h(23)}
Signatures:	s({h(1), h(2), h(4), h(5), h(6)})	s({h(7), h(8), h(9), h(12)})	s({h(14), h(15), h(16), h(18)})	s({h(19), h(21), h(22), h(23)})

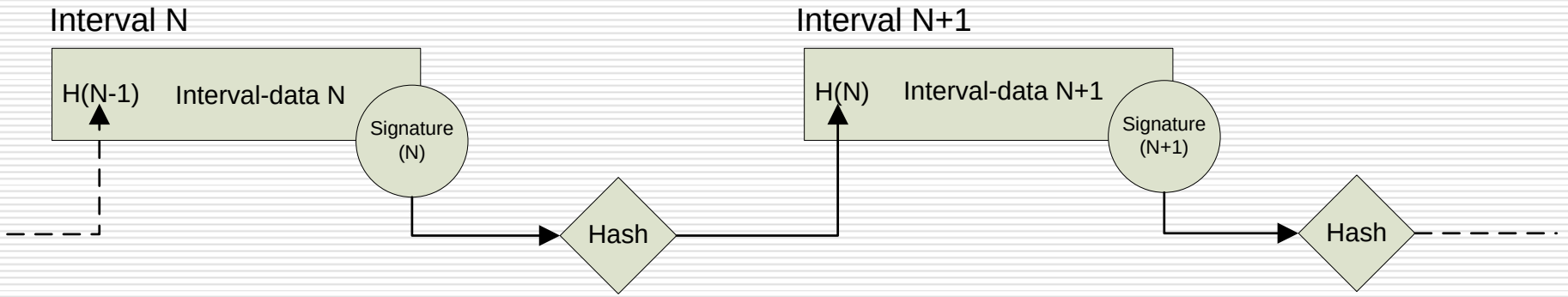
(Hier ist nur ein Kanal bzw. eine Richtung dargestellt)

Vorteile

- Effizienzgewinn
  - Bei Intervalllängen von 1-2s wird das kontinuierliche Signieren auch mit langsamer Hardware (z.B. Smartcard) möglich
  - Speicherbedarf für Puffer beträgt nur Größe eines Intervalls
- Temporäre Reihenfolge innerhalb eines Intervalls wird durch Signatur geschützt.
- Skalierbar: Intervalllänge einstellbar, Tradeoff zwischen Sicherheit und CPU-Last

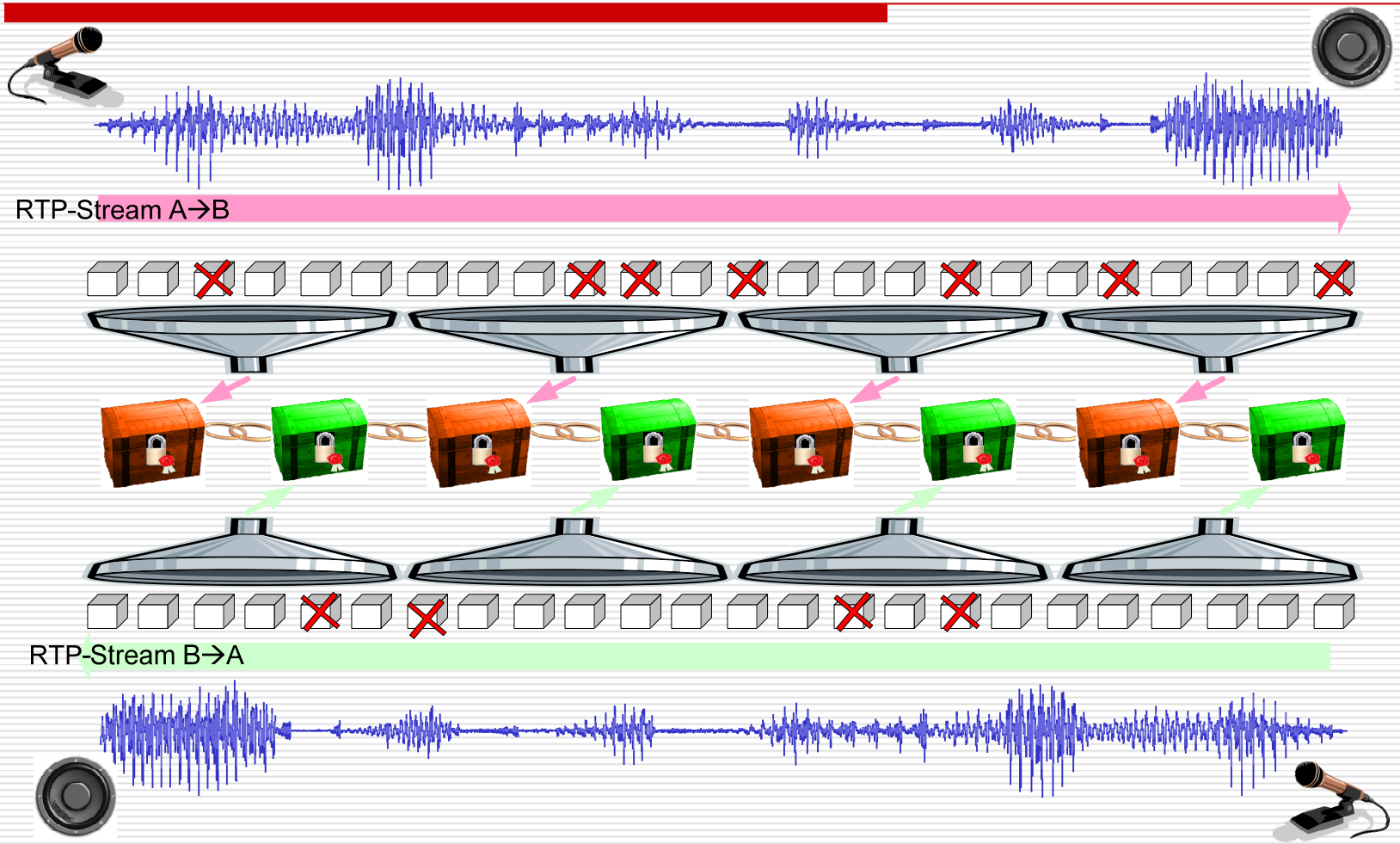
Intervallverkettung zur Sicherung der zeitlichen Kohäsion





➔ Angreifer kann weder Gesprächspassagen entfernen, noch die Reihenfolge verändern

Schützen der Bidirektionalität



Alternierend Intervalle von beiden Richtungen verketten

➔ Beide Richtungen sind untrennbar miteinander verwoben

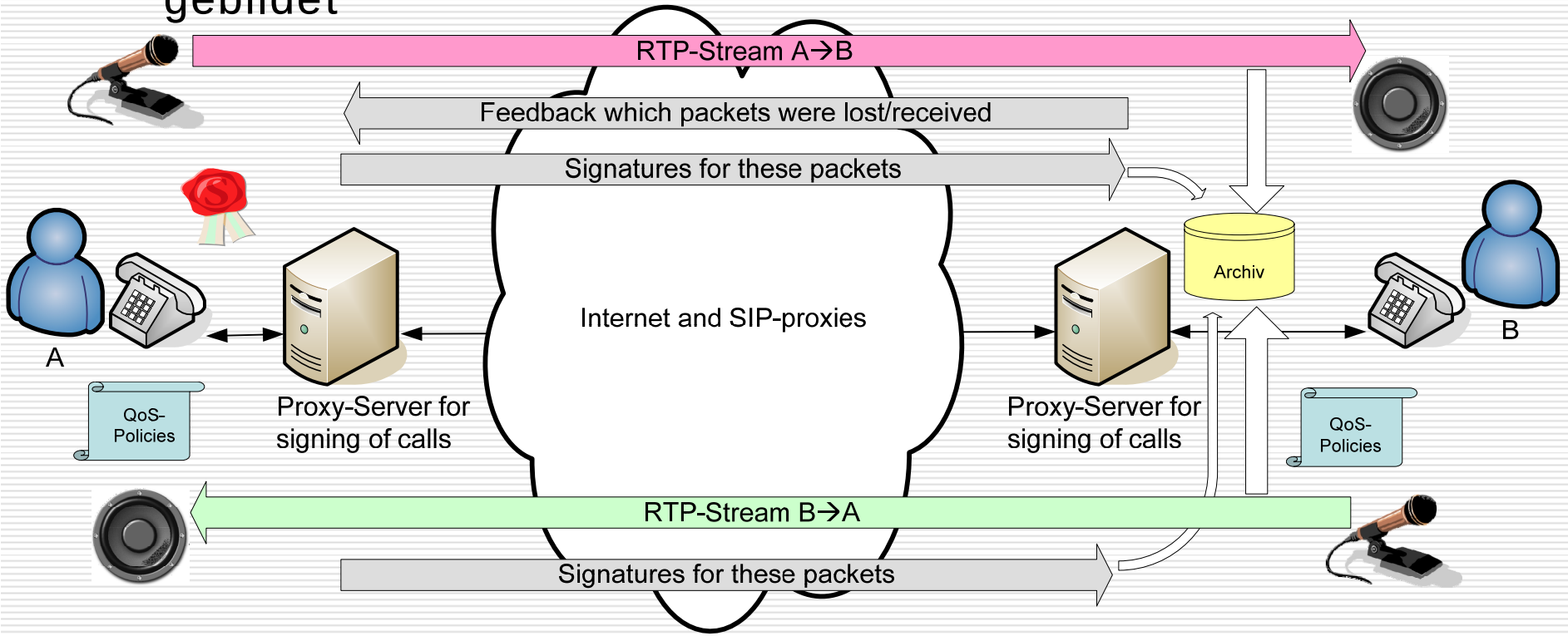
Umgang mit Packet-Loss

- Wie in Einleitung gesehen:
  - Packet Loss typisch für VoIP
  - Einige Codecs können es ausgleichen
  - Bestimmte Menge Packet Loss beeinträchtigt Verständlichkeit nicht
- Signaturen dürfen nicht ungültig werden, wenn ein Paket beim Transport verloren geht (im Gegensatz zu im Archiv)
- Nur das signieren, was auf Gegenseite angekommen ist

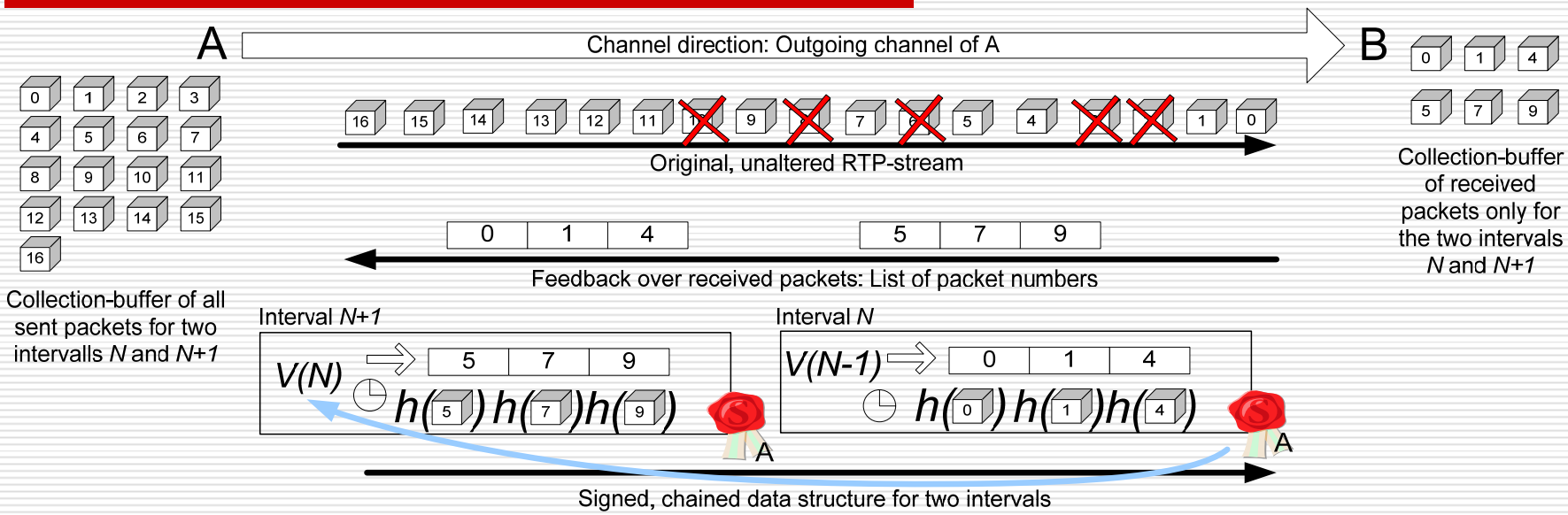
➔ Feedback-System, basierend auf Intervallen

Feedback-System

- RTP-Pakete werden ohne Verzögerung durchgereicht
- Signaturbildung durch A, Signaturversand A→B und Prüfung durch B erfolgen verzögert (1-2 Intervalllängen)
- Signaturen werden nur für die nicht verlorenen Pakete gebildet



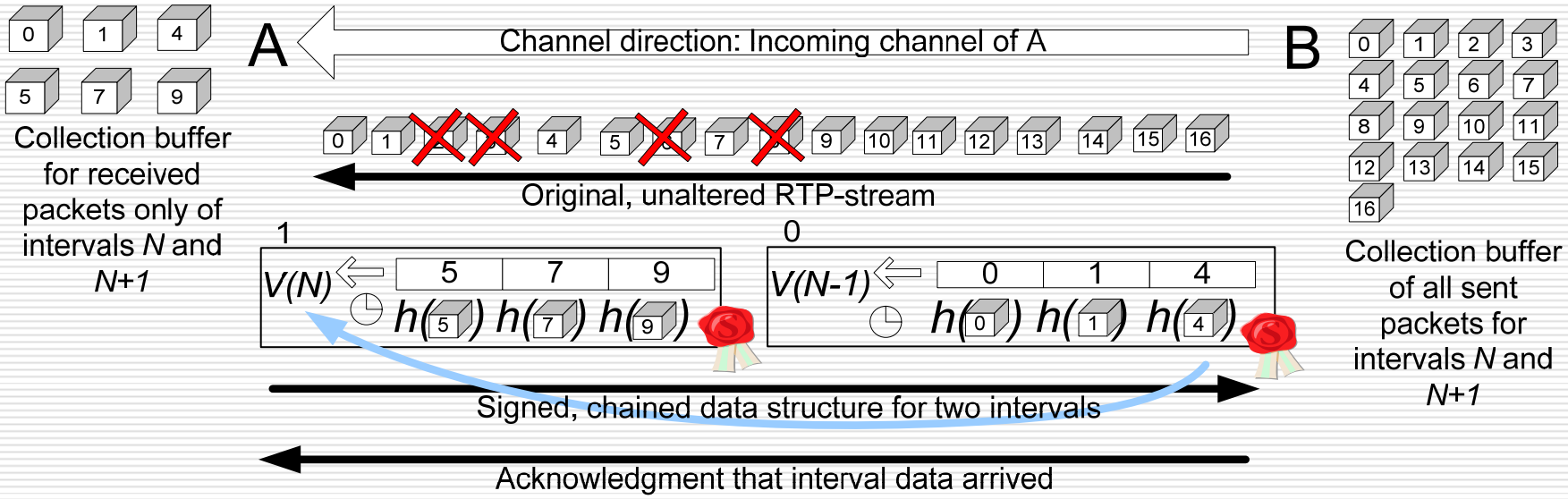
Protokoll A→B



V(N), V(N-1)	Chaining-values (hashes) of the preceeding interval	Lost packet	Date/time of interval
h( )	Hash-function	Signed data	Direction: {A→B, B→A}

- Pakete werden auf beiden Seiten in Puffern gesammelt.
- B sendet nach jedem Intervall eine Liste der tatsächlich empfangenen Pakete
- A bildet für diese Pakete Hashwerte und signiert die (kleinen) Intervalldaten und sendet sie an B

Protokoll B→A

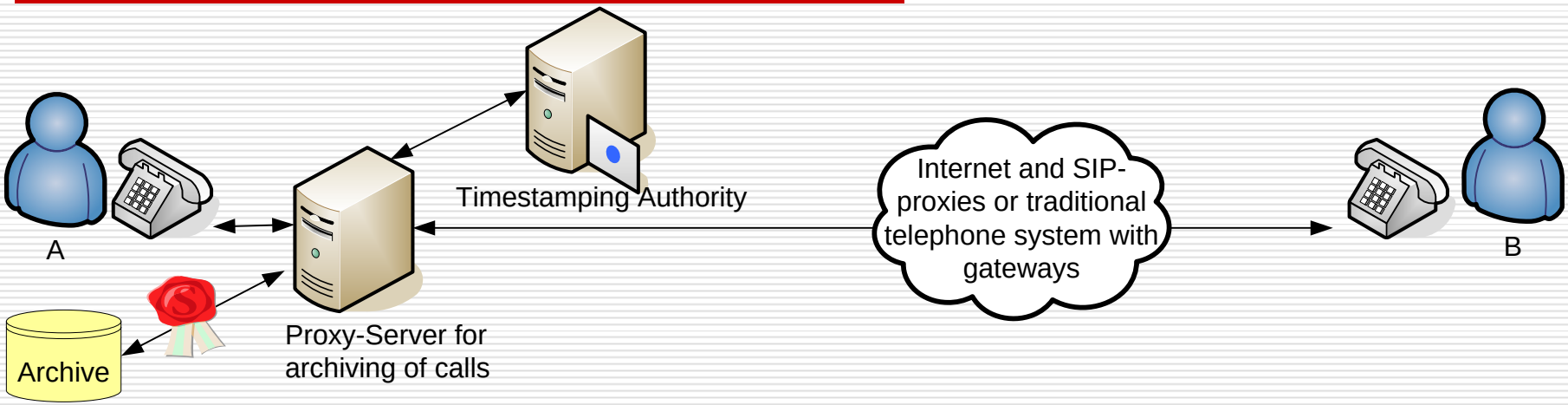


- A generiert für die Pakete von B, die bei A angekommen sind, Signaturen

QoS Policies

- Einige Angriff basierend auf Quality of Service und insbesondere Paketverlust sind denkbar:
  - Das Verfahren nimmt explizit Rücksicht auf Paketverlust und signiert nur, was die Gegenseite angibt empfangen zu haben
  - Wenn die Gegenseite lügt, kann sie unvorteilhafte Passagen des archivierten Telefonats unterdrücken, da dann so wenige Pakete signiert und archiviert werden, dass es vor Gericht später unverständlich wird
  - Semantisch hat der Gesprächspartner es jedoch vollständig verstanden und ist im Glauben, die Bemerkung würde archiviert
- ➔ Permanente Überwachung des QoS der Verbindung: Bei zu hoher Paketverlustrate (>5%) wird das Gespräch je nach Policy vom Proxy abgebrochen oder nur das Signieren beendet
- A und B prüfen für jede Intervalllisten bzw. Signaturpaket die Paketverlustrate. QoS-Probleme können innerhalb 2x Intervalllänge erkannt werden, einem Angreifer bleibt nur wenig Zeit für Fälschungen bevor diese erkannt werden
- Außerdem wird geprüft, ob die Intervalle zeitlich zu ihren Vorgängern und dem anderen Kanal passen

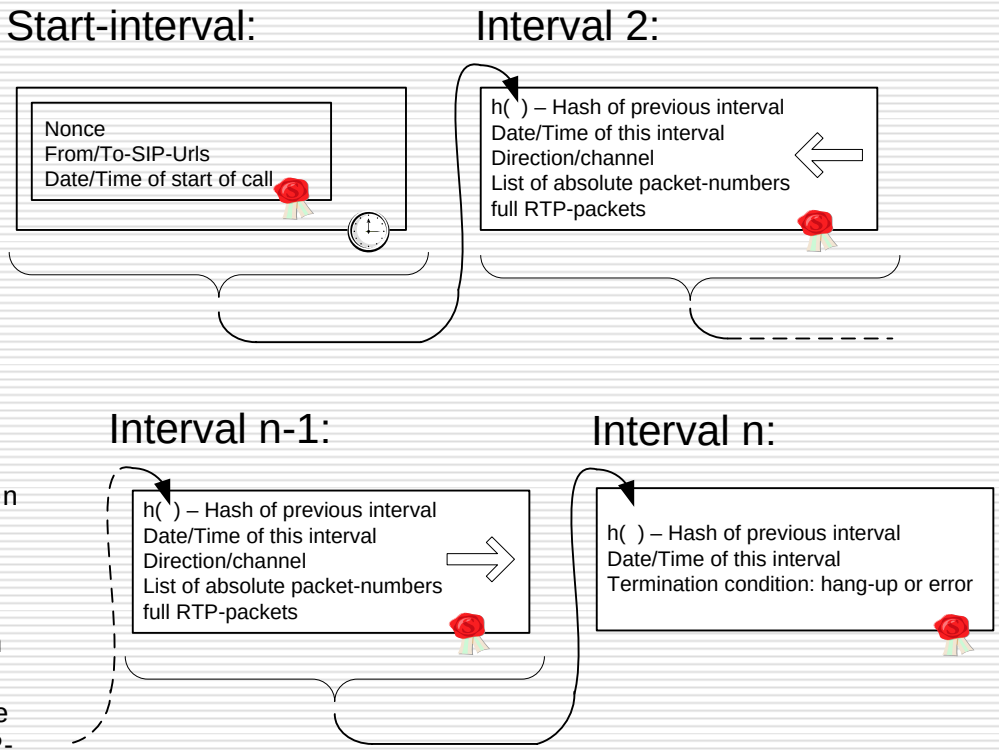
Archiv Szenario



- Erfordert im Gegensatz zum Signierszenario keine Modifikationen an End-geräten: Nur ein Teil der Strecke von A nach B muss auf SIP/RTP basieren.
- Einsatz bei sicherheitskritischen Anwendungen wie Telefon-Aktienhandel oder Call Centern.
- Sichert Gespräch kontinuierlich und nicht wie beim Stand der Technik als Dokument.
- Da die Sicherung mit Beginn des Gesprächs anfängt und der Beginn durch einen zusätzlichen vertrauenswürdigen Zeitstempel gesichert wird, müsste ein erfolgreicher Angreifer in der Lage sein, Manipulationen innerhalb eine Intervallzeitraums in Echtzeit durchzuführen

Datenformat für archivierte Telefonate

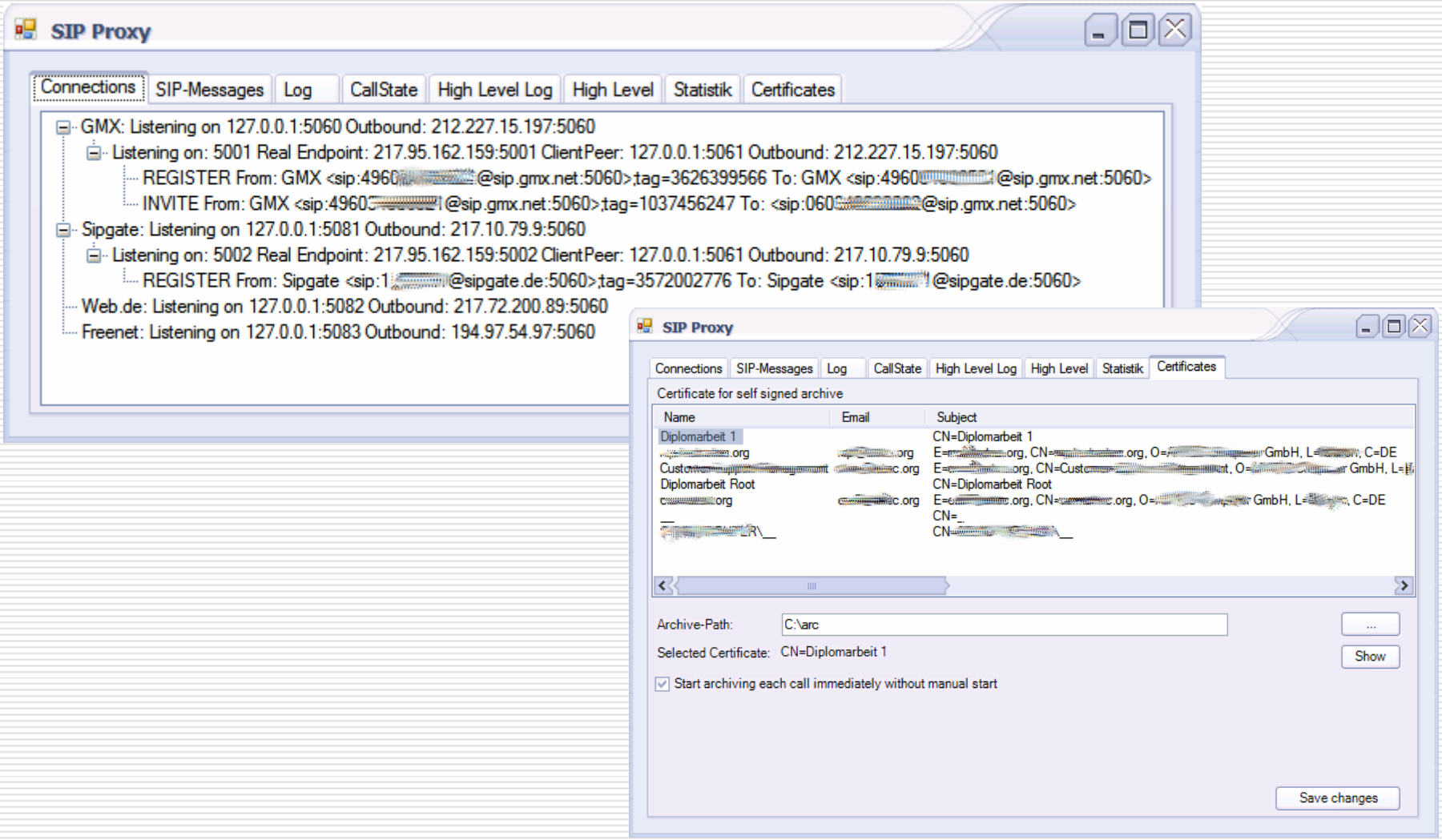
- Die Intervalle werden mit dem PKCS#7 Signed Envelope Standard und dem privaten Schlüssel des Archivs signiert.
- Erstes Intervall:
  - Enthält SIP-ULRs von Anrufer und Angerufenen
  - Enthält Datum und Uhrzeit des Anruf-Beginns
  - Enthält Abbildung RTP-Payloads auf Codecs und Parameter
  - PKCS#7 Kontainer enthält gesamte Zertifikatskette (kann dafür in allen folgenden Intervallen entfallen)
  - Wird zusätzlich mit einem Timestamp versehen
- Reguläre Intervalle
  - Stammen entweder vom Kanal A→B oder der anderen Richtung
  - Speichern Flag für Richtung/Kanal
  - Speichern Zeitpunkt des Intervalls
  - Enthalten eine Liste mit absoluten Sequenznummern der Pakete, die das Archiv gesehen hat
  - Enthalten die kompletten RTP-Pakete, die in der Liste aufgezählt sind, zusammen mit abgeschnittenen RTP-Timestamps und Sequenznummern
- Abschließendes Intervall:
  - Grund des Gesprächsabbruchs: z.B. reguläres Auflegen durch A oder B, Verletzung der QoS-Kriterien, Erkennung von Manipulationen
  - Zeitpunkt des Gesprächsendes



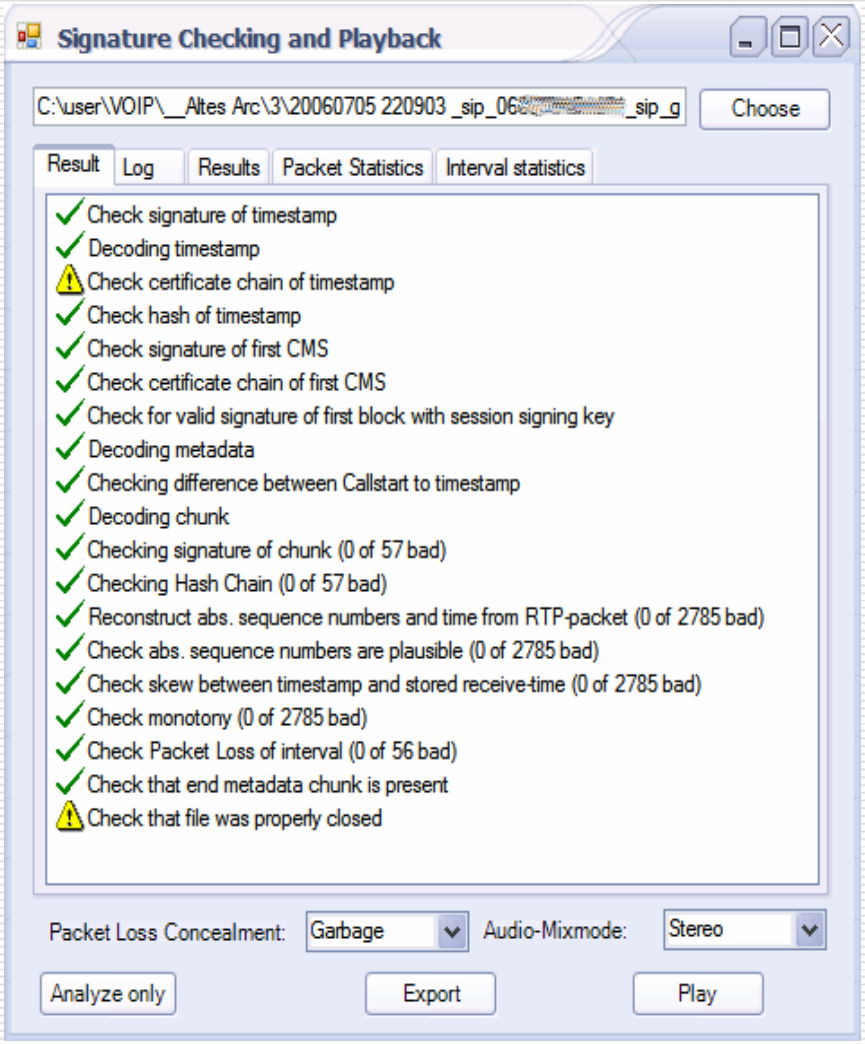
Was wurde im Demonstrator implementiert?

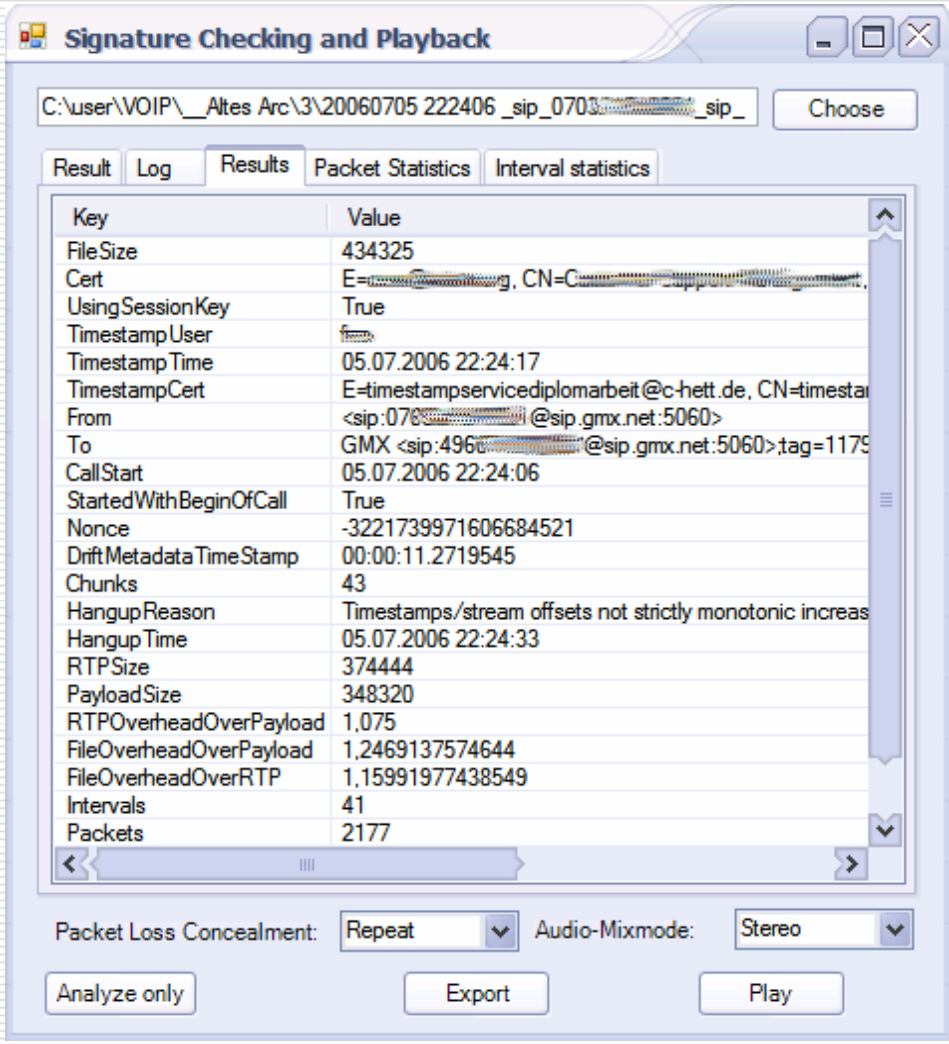
- Protokolle und Parser: SIP, SDP, RTP, Codec G.711, STUN, WAV
- SIP-Proxy, der mehrere Gespräche gleichzeitig verwalten und RTP-Ports auf sich umbiegen kann
- Mehrere Verfahren, um einen zweiten Datenkanal für Signaturen aufzubauen
- Selbst-Signiertes Archiv als Plugin für Basis-Proxy:
  - Intervallbildung und –verkettung
  - Replay-Window
  - QoS-Messungen, Policys und Visualisierung
  - Verwebung beider Kanäle
  - Timestamp-Server und Client
  - PKCS#7 Signaturen und Zertifikatsbehandlung
  - Datenformat
- Prüf- und Abspielprogramm für archivierte Telefonate
  - Nur Prüfen, Export als WAV, Abspielen
  - Mix beider Kanäle
  - Prüfen auf korrekte Verkettung, Signaturen, Zertifikate, Hash-Werte
  - Visualisierung und Prüfung des Packet-Loss

Screenshots Proxy

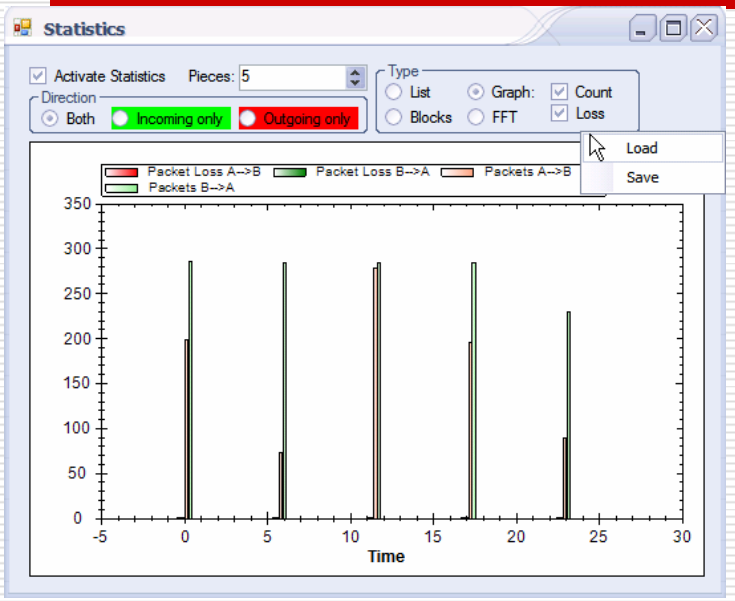


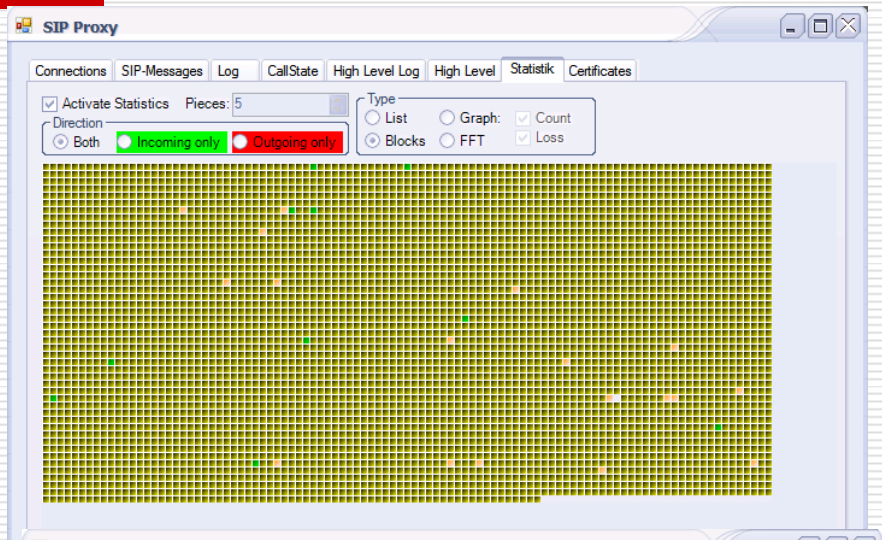
Screenshots Prüftool

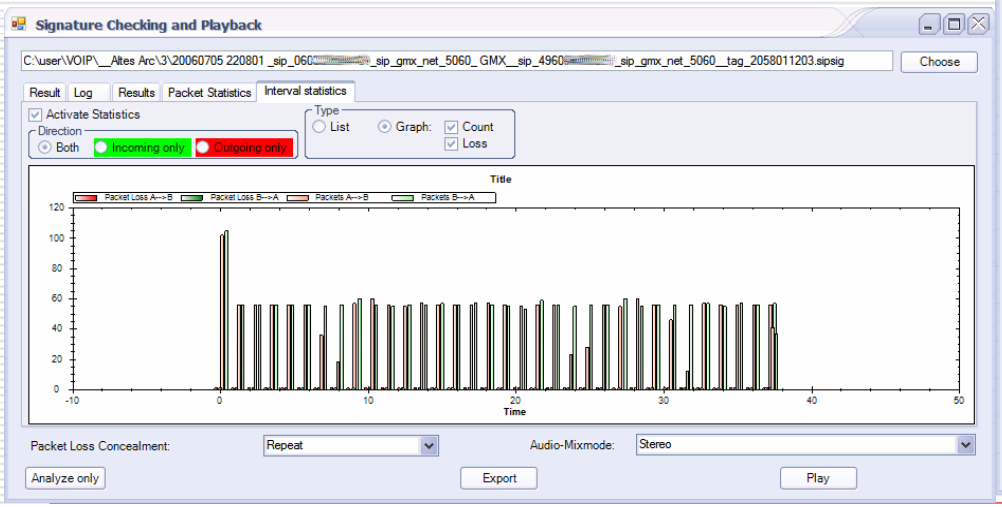


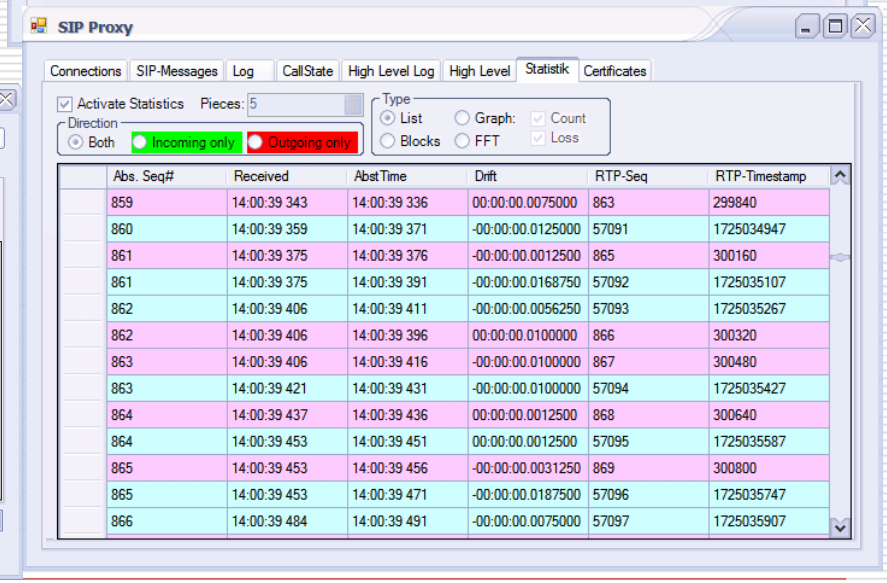


Screenshots Statistik









Abs. Seq#	Received	Abst Time	Drift	RTP-Seq	RTP-Timestamp
859	14:00:39 343	14:00:39 336	00:00:00.0075000	863	299840
860	14:00:39 359	14:00:39 371	-00:00:00.0125000	57091	1725034947
861	14:00:39 375	14:00:39 376	-00:00:00.0012500	865	300160
861	14:00:39 375	14:00:39 391	-00:00:00.0168750	57092	1725035107
862	14:00:39 406	14:00:39 411	-00:00:00.0056250	57093	1725035267
862	14:00:39 406	14:00:39 396	00:00:00.0100000	866	300320
863	14:00:39 406	14:00:39 416	-00:00:00.0100000	867	300480
863	14:00:39 421	14:00:39 431	-00:00:00.0100000	57094	1725035427
864	14:00:39 437	14:00:39 436	00:00:00.0012500	868	300640
864	14:00:39 453	14:00:39 451	00:00:00.0012500	57095	1725035587
865	14:00:39 453	14:00:39 456	-00:00:00.0031250	869	300800
865	14:00:39 453	14:00:39 471	-00:00:00.0187500	57096	1725035747
866	14:00:39 484	14:00:39 491	-00:00:00.0075000	57097	1725035907