# All for one and one for all - Trusted Identity Security

**Chris Wendt** - Director Technical R&D, IP Communications, Comcast
Co-Chair IP-NNI Joint Task Force and Co-Chair STI-GA Technical Committee

# STIR/SHAKEN -
# Party is in full swing

- RSVPs have been received
- Guest’s have (mostly) arrived
- Drinks and hors d’oeuvres are ready

- The tokens are hot and ready to be consumed 😛


ALL YOU NEED IS MOTIVATION
FALSE: YOU NEED FEAR AND AN APPROACHING DEADLINE
memegenerator.net

# STIR/SHAKEN - All dressed up and ready to go

Now what?

By Attributed to William Segar - http://www.artfund.org/what-to-see/exhibitions/2013/10/10/elizabeth-i-and-her-people, Public Domain

# Are we dancing?  or still figuring things out?

By Wilhelm Gause - Historisches Museum der Stadt Wien [1], Public Domain

# We have the framework in place

The dresses, the shoes

We need to learn the

**ART**

**STYLE**

By Edgar Degas - https://www.vogue.fr/fashion-culture/article/edgar-degas-and-the-dancer-the-artists-most-beautiful-representations, Public Domain

# Move from fundamentals to mastery

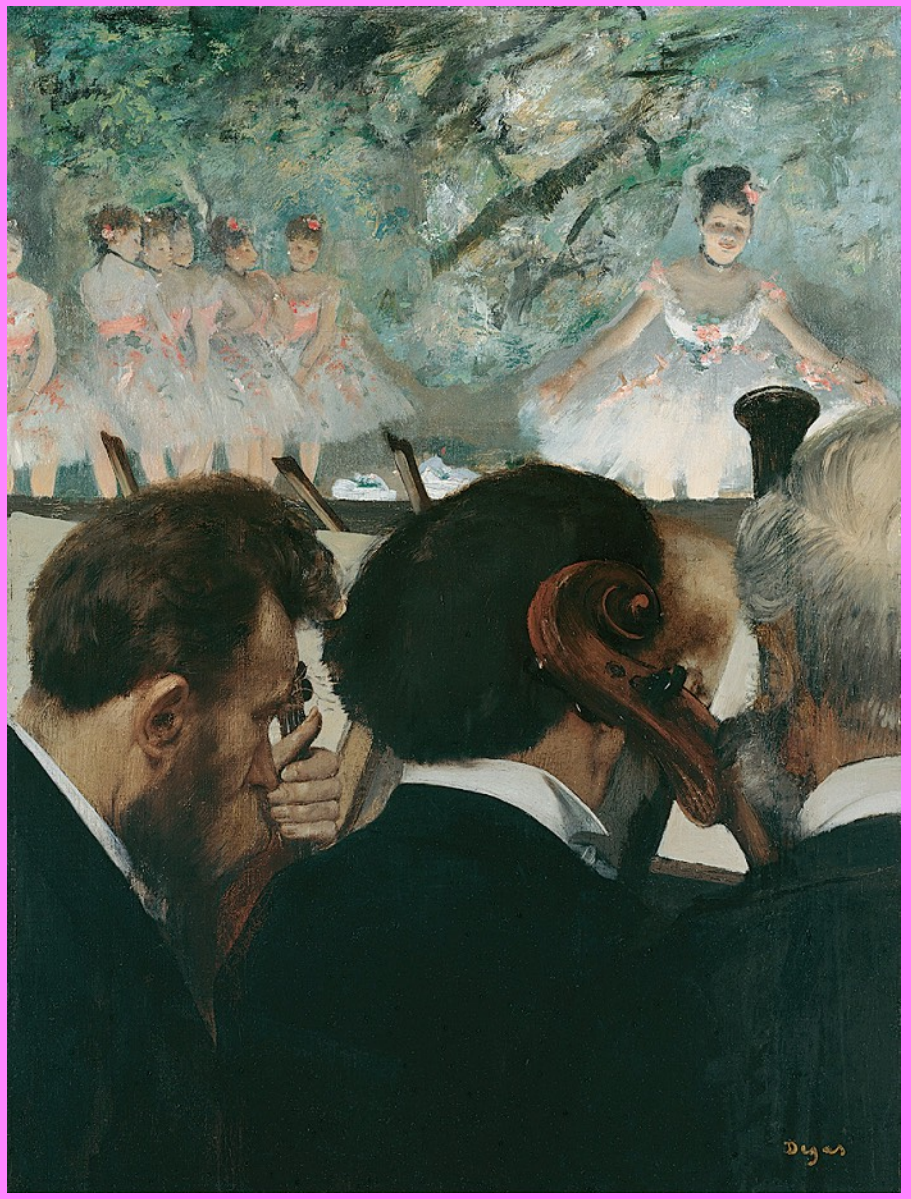
By Edgar Degas - https://www.vogue.fr/fashion-culture/article/edgar-degas-and-the-dancer-the-artists-most-beautiful-representations, Public Domain

# Move from fundamentals to mastery

Going through the motions

vs

A master performance




By Edgar Degas - BQE2l6uLmNmnMA at Google Cultural Institute, zoom level maximum, Public Domain

# Identity security is not only about crypto/digital signatures

Largely about the

**TRUTH and TRUST**

associated with the

**information/**

**identity**

being brought into

the system

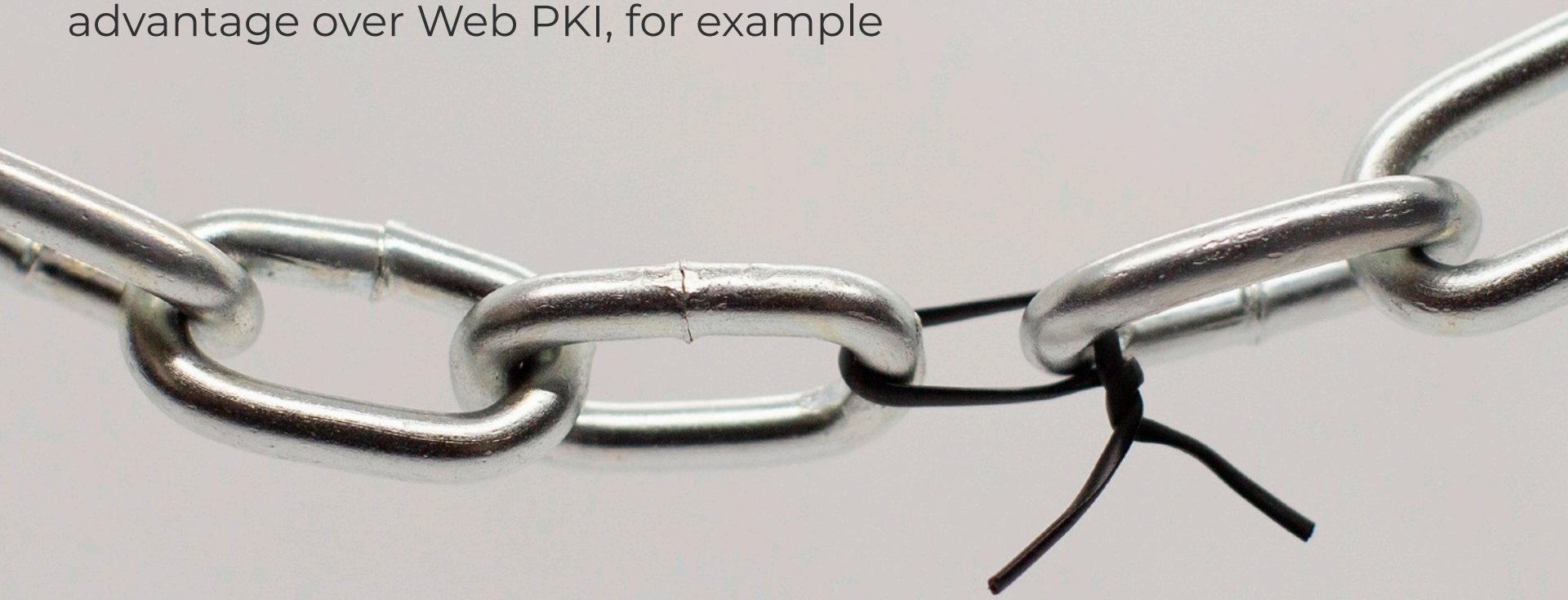

By Renaud d'Avout - Own work, CC BY-SA 3.0

Security is only as strong as the weakest link

The **weakest link** for STIR/SHAKEN is not necessarily related to signatures or credentials or certificates

It’s related to the **accuracy** and **implicit trust** that consumers of the telephone network depend on

Securing identity in the telephone network has an **inherent** advantage over Web PKI, for example



Participants play within a regulated system where STI-GA/PA governed certificates are issued to a **limited number** of **well-known and approved** entities with **incentive** to stay in that eco-system

# Trusted identity needs to be end-to-end

- **Retail service**: calling device authentication relationship is direct
    - OSP directly authenticates device used to place the call in their network
- **Everything else**: calling device authentication relationship is indirect
    - “End-to-end” starts with authenticating the caller and carrying that through end-to-end
- Fundamental requirement we have is:

By Unknown author - http://history.scps.ru/musket/02.htm, Public Domain

**Non-repudiation:** the assurance that the owner of a signature key pair that was capable of generating an existing signature corresponding to certain data cannot convincingly deny having signed the data.

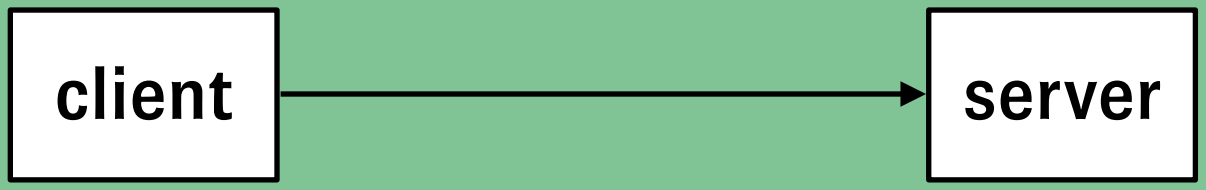
# Telephone Service is an Application

- Not just routing packets to the right place
- The sooner we recognize this the easier we will get to **TRUST**
- Authentication inherently begins at the **device** that initiates a call and is carried throughout the transaction end-to-end
- SIP is hop-by-hop, a bit different than client/server based protocols
- But that is why it's even MORE important to enforce end-to-end

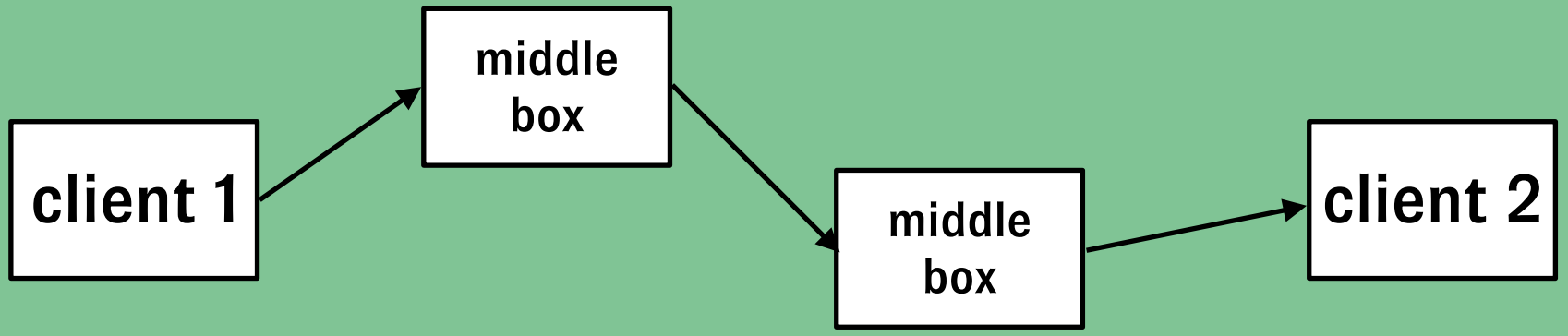
By Richard Knötel - http://warfare.tk/Ottoman/Ottoman.htm, Public Domain

# Authentication/Trust

## Traditional Web Authentication (HTTPS)




## SIP/STIR Model

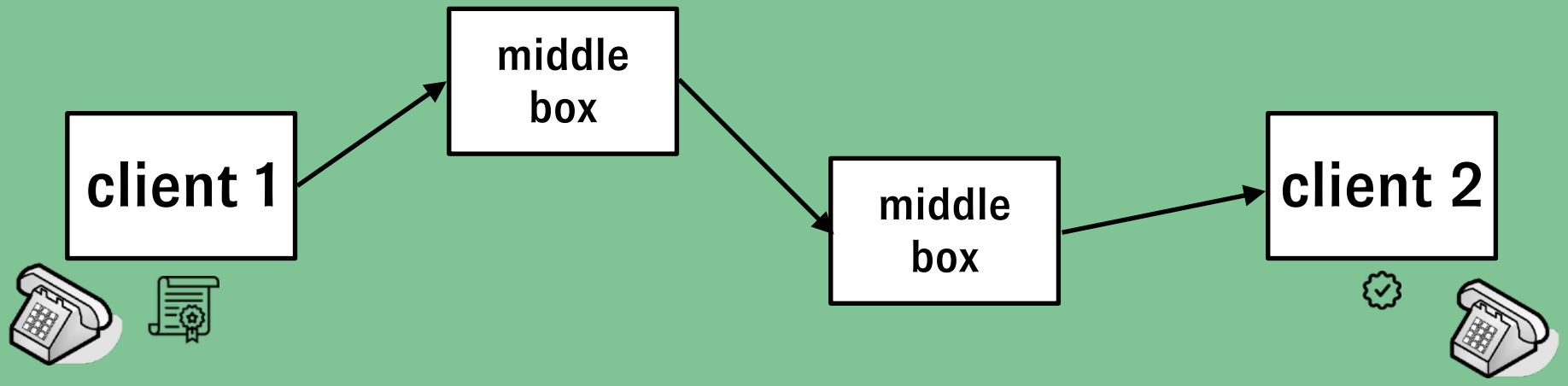



Trust in hop-by-hop model MUST traverse middle boxes

# Authentication/Trust End-to-End

## Traditional Web Authentication (HTTPS)

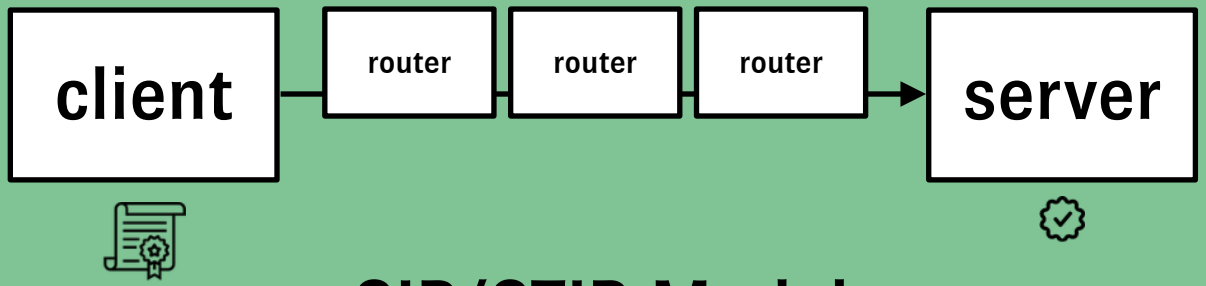

## SIP/STIR Model



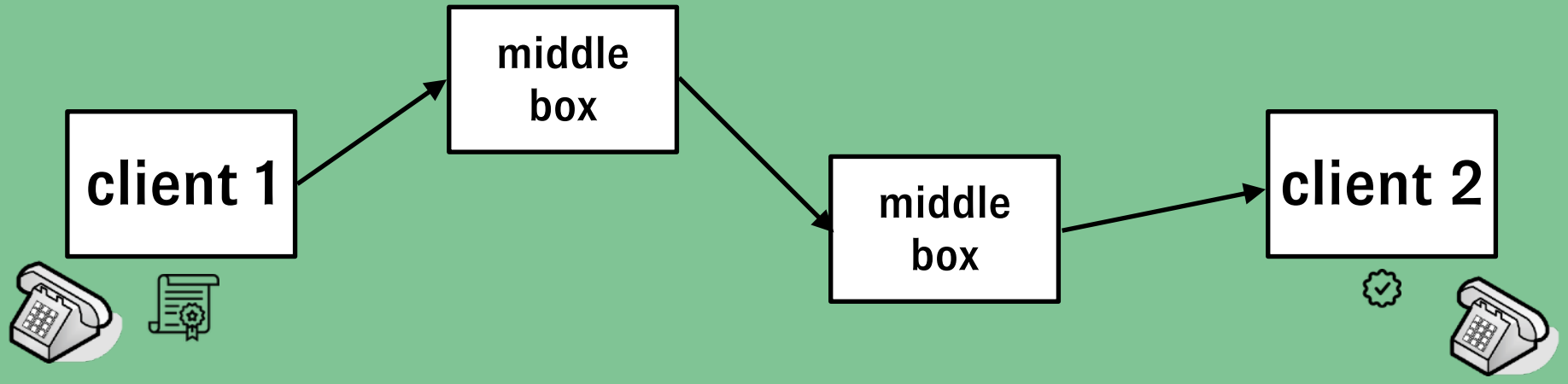

Trust in hop-by-hop model MUST traverse middle boxes from where the call was authenticated

# Authentication/Trust End-to-End

## Traditional Web Authentication (HTTPS)



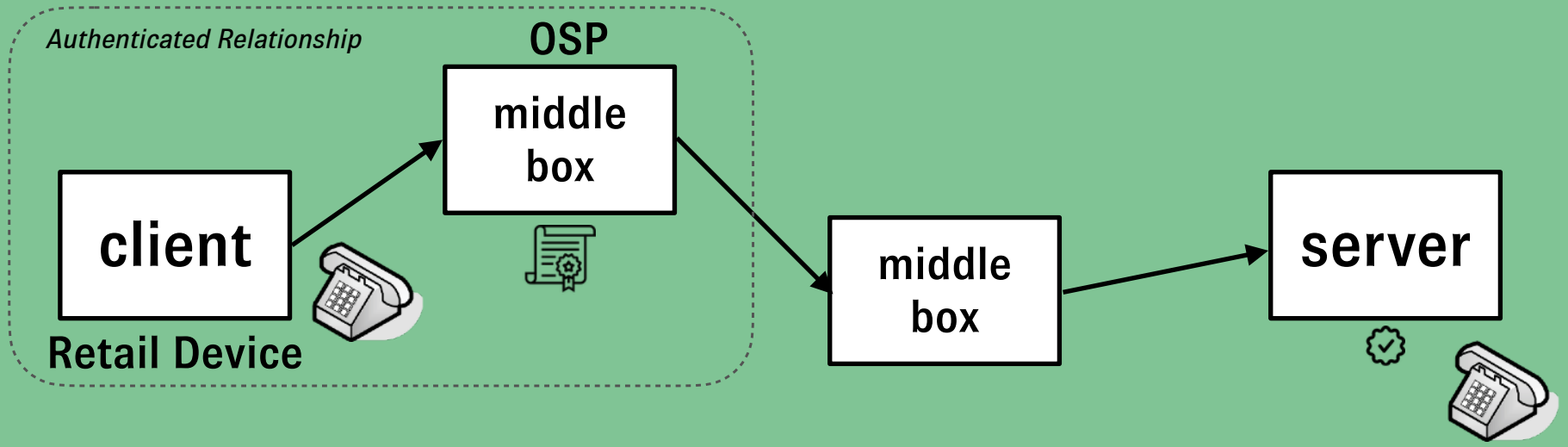

## SIP/STIR Model



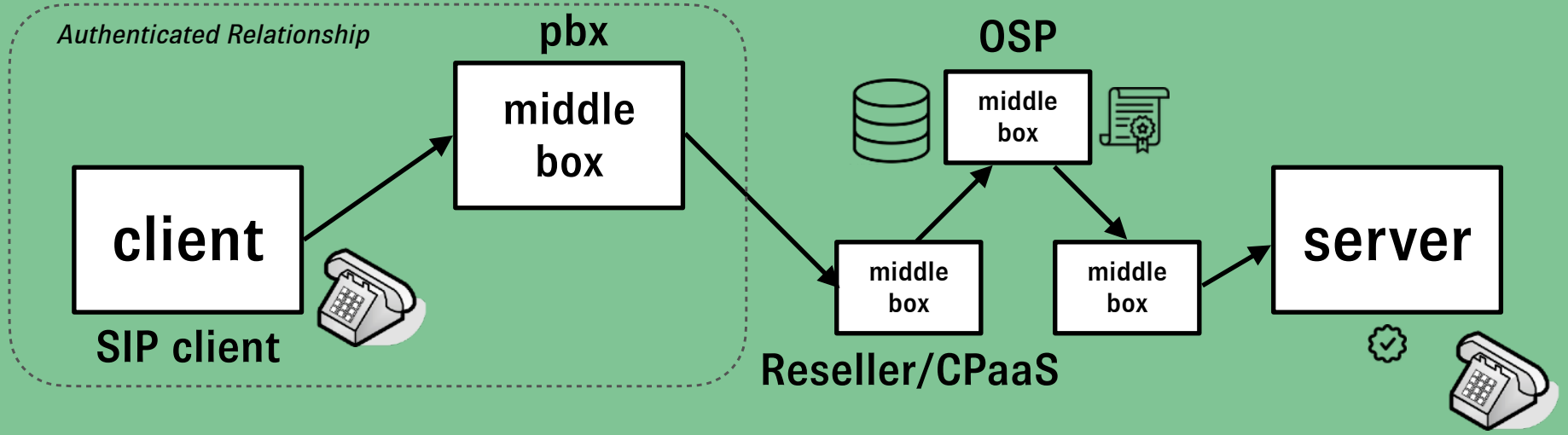

Internet/IP model is hop-by-hop but we never think about that at application layer

# Authentication/Trust

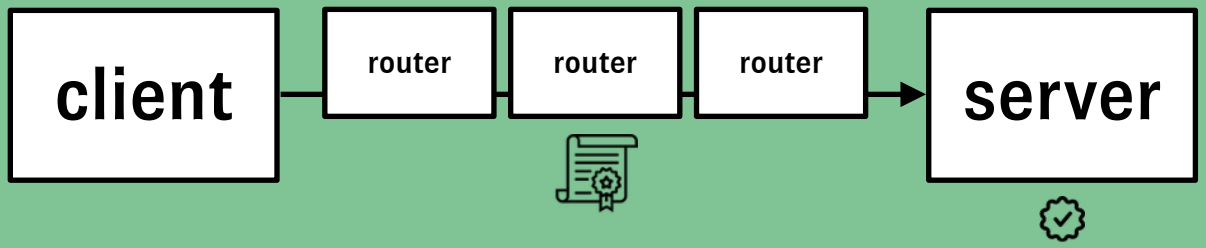
## Retail Model with SHAKEN attestation model



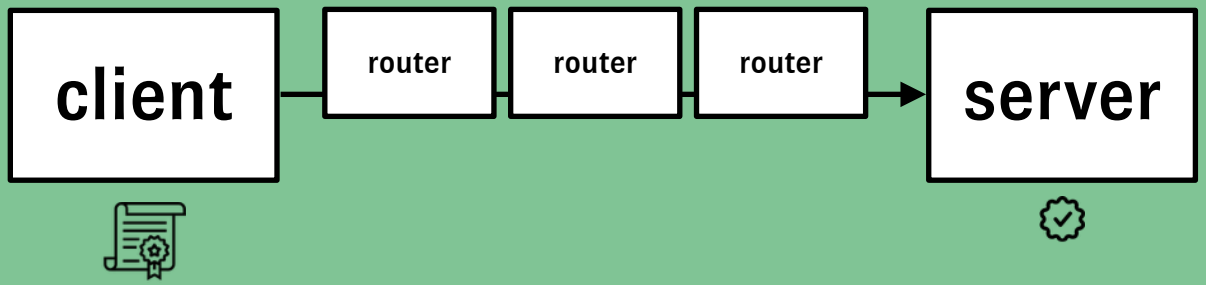

## Enterprise Model with SHAKEN attestation model



# Authentication/Trust End-to-End

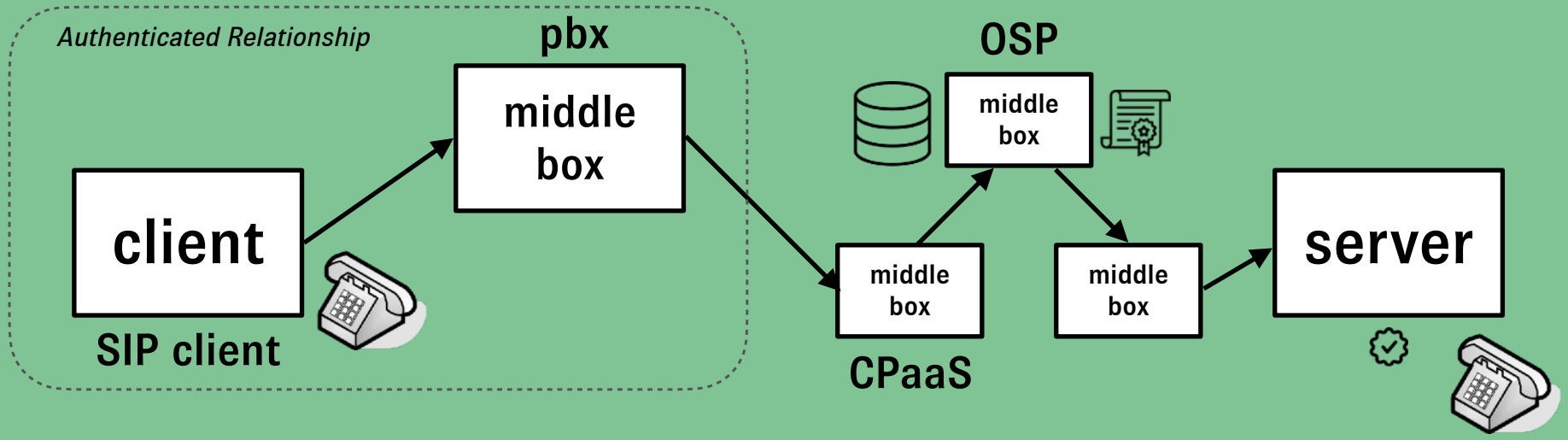


# Authentication/Trust End-to-End

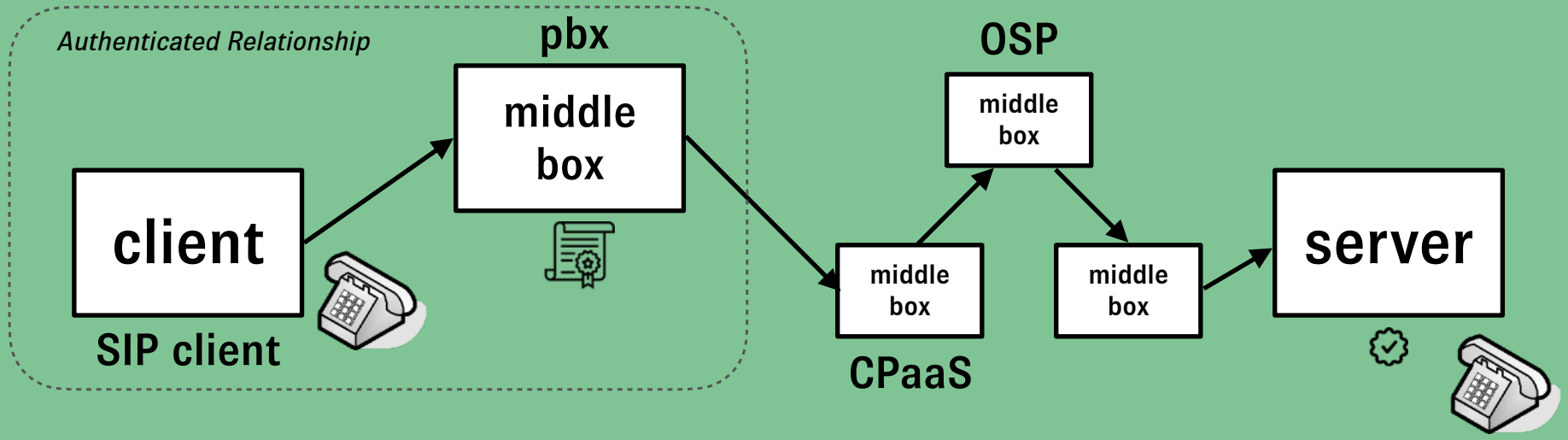


# Authentication/Trust

## Enterprise Model with SHAKEN attestation model




## Enterprise Model with TN Cert model



# Distributed Trust

- The telephone network just like IP networks or globally the internet is a **distributed model**.
- Network to network interconnection / hop-by-hop relationships
- Trust must be **distributed** and **cooperative**
- Authentication is about trust that you are who you say you are because you have been vetted (Extended validation :: CATA model)
- It's real-time and session based and must be independent of how a call is routed and who the callee is.

Musketeers in China, Public Domain

# Trust in the eco-system

- Trust is key
- Again, we have fundamental **technology/ crypto in place**
- It's about maintaining an eco-system of
    - **accountability**
    - **incentives**
- where the bar is maintained high, back-stop of STI-GA policy and regulatory (and if necessary criminal) enforcement
- so if a signature/identity is validated
- there is a level of inherent trust, most importantly to end-users, because the eco-system is healthy

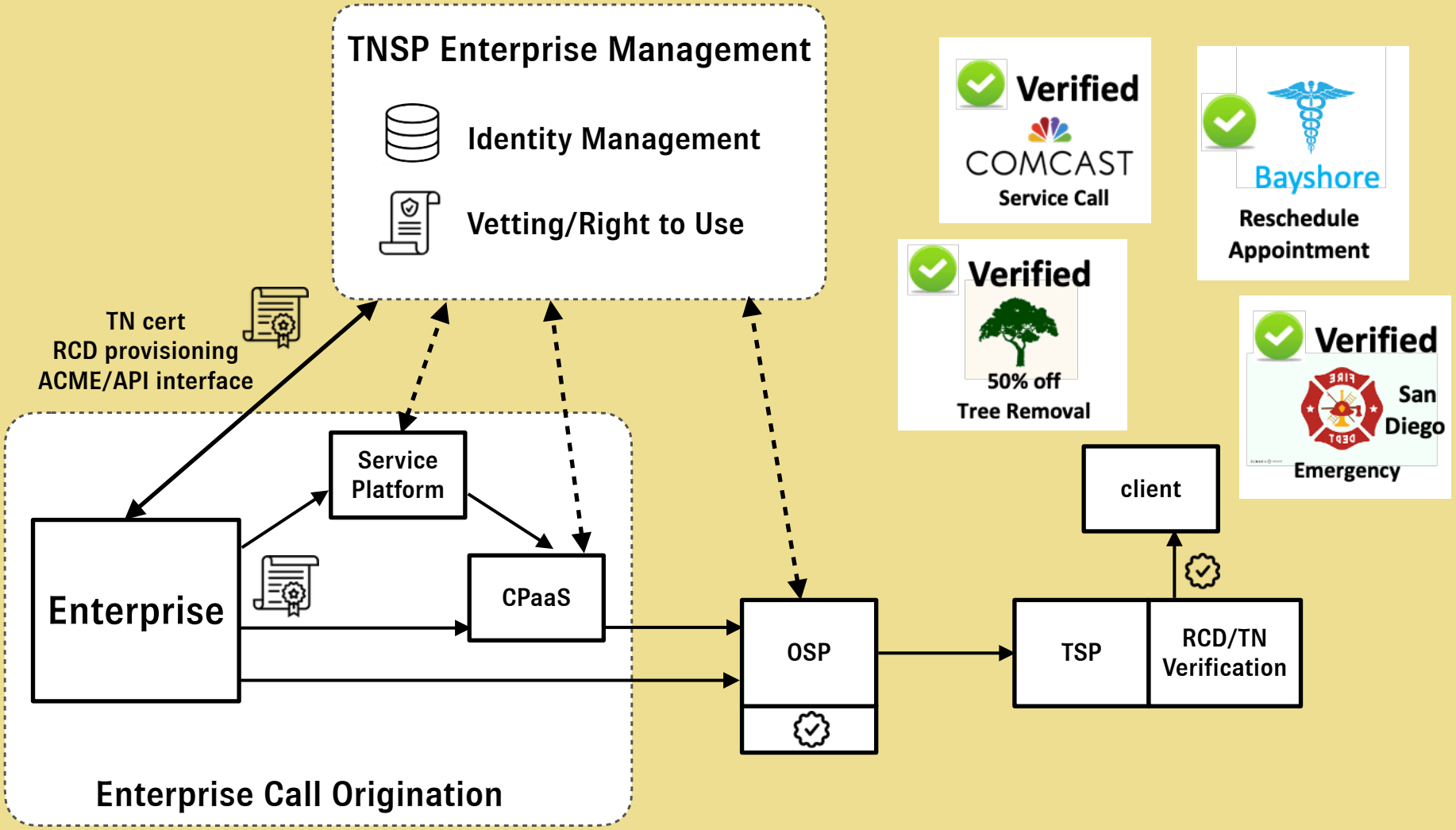
A painting of a Mughal infantryman. by Unknown (production) - https://collections.vam.ac.uk/item/O432817/drawing-a-mughal-infantryman/, Public Domain

# How do we enforce trust?

- Start with the authenticated device relationship, the initiation of a call
- **Retail**: Vetted customers and their use of assigned telephone numbers
    - Rinse, Repeat (we got this)
- **Enterprise**:
    - Vet customers
    - Manage use of telephone numbers
        - Directly assigned
        - Bring your own numbers (i.e. spoofed)
    - Sign call with TN cert
    - Downstream consumption OSP, TSP, end-user can trust with confidence

By Unknown author - Историческое описание одежды и вооружения российских войск, под ред. Висковатова А.В., Часть 1. — СПб. : Воен. тип., 1841-1862.— Илл. 108, Public Domain

# Enterprise Service Scenarios



# How do we enforce trust end-to-end

# How do we enforce trust end-to-end

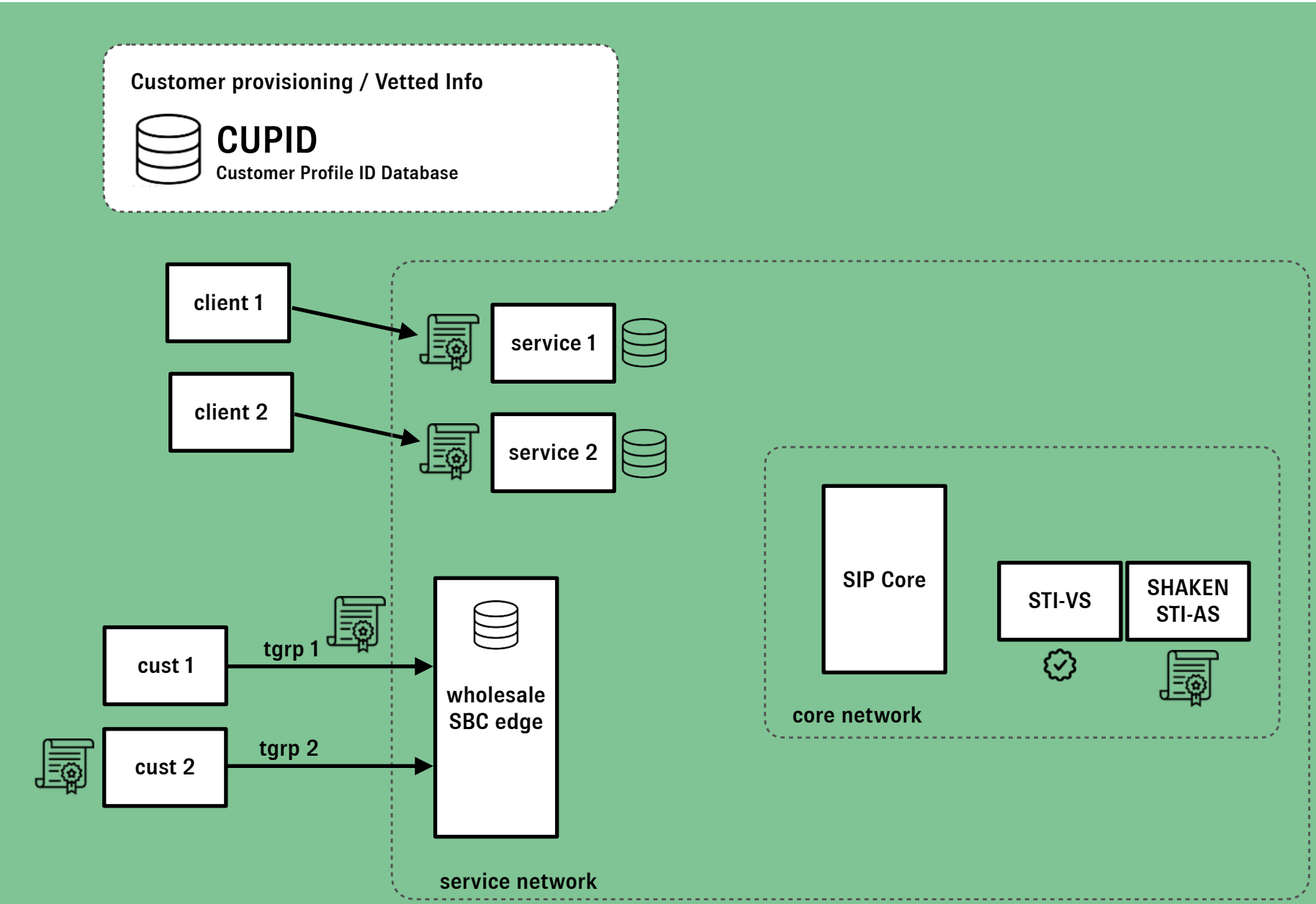
Use TN based delegate certificates

# How do we enforce trust end-to-end

Use TN based delegate certificates

# Questions?

# Enforce trust end-to-end

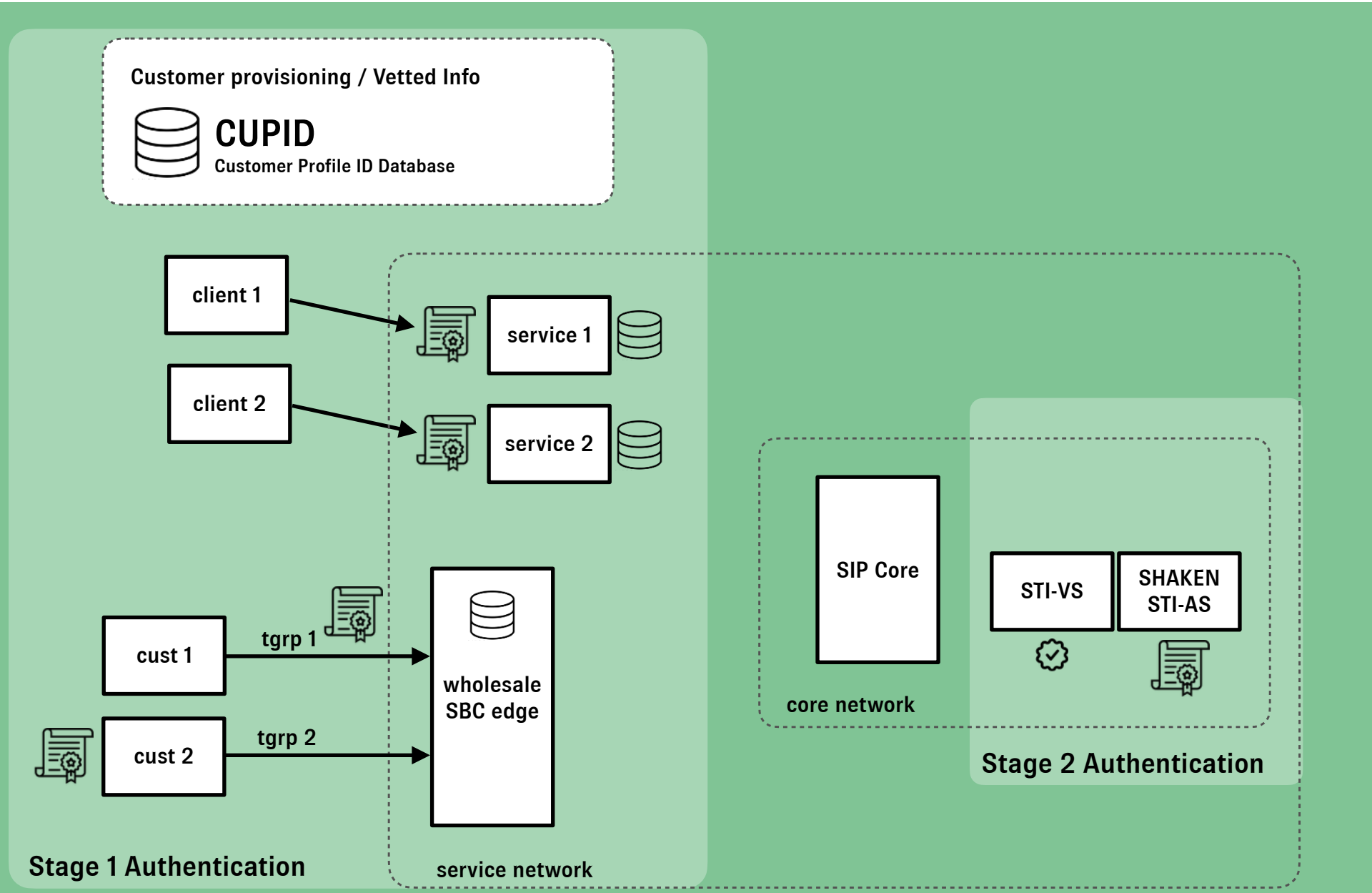


# Enforce trust end-to-end

| Customer Profile Table | | | | | |
|---|---|---|---|---|---|
| **CP-Index** | **Customer** | **Assigned TNs** | **Customer Policies** | **Rich Call Data** | **Signing Credentials** |
| service-1 | default | -- | policyList-1a | -- | Del-cert-1 |
| | customer-1 | TN List 1 | policyList-1b | vetted rcd info for customer-1 | Del-cert-2 |
| | customer-2 | TN List 2 | policyList-1c | vetted rcd info for customer-2 | Del-cert-3 |
| | customer-3 | TN List 3 | policyList-1d | vetted rcd info for customer-3 | Del-cert-4 |
| service-2 | default | -- | policyList-2a | -- | Del-cert-5 |
| | customer-4 | TN List 4 | policyList-2b | vetted rcd info for customer-4 | Del-cert-6 |
| | customer-5 | TN List 5 | policyList-2c | vetted rcd info for customer-5 | Del-cert-7 |
| tgrp-1 | customer-6 | TN List 6 | policyList-3a | vetted rcd info for customer-6 | Del-cert-8 |
| tgrp-2 | customer-7 | TN List 7 | policyList-4a | vetted rcd info for customer-7 | Del-cert-9 |

- Populated via billing and provisioning processes
- Contains TN or trunk group level information
- Contains Vetted information triggering RCD
- Supplements internal service information/provisioning
- Important: only contains vetted/provisioned info we sign for (our direct customers)
- We want to receive authenticated calls through wholesale/transit relationships

# Enforce trust end-to-end - two stage approach



# Enforce trust end-to-end - two stage approach

- **Stage 1 Authentication**
  - Signing with TN cert or trunk group cert at point of service authentication or next hop
  - If vetted info is available, sign with TN cert/RCD
  - Apply service policies based on vetted customer data
  - If service association is available sign with trunk group cert
- **Stage 2 Authentication**
  - Calls are routed through network normally landing on SIP core for routing to NNI
  - Calls signed with TN cert are signed with SHAKEN attest = “A”
  - Calls signed with trunk group cert are signed based on CUPID assigned policy
  - Calls not signed receive “C” attestation

# Enforce trust end-to-end - two stage approach

- **Why two stages?**
  - As explained, maintains a key property of trust, **signing the call at the point of service authentication**
  - Associates subscriber identity(s) and potential RCD info at the point where it's **naturally provisioned** (**as part of a service, not routing function**)
  - **Separation of authentication and SHAKEN attestation** allows for independence of network routing, once identity header is added, SIP routing doesn't matter until it exits SP network
  - No matter where 1st stage authentication is performed, or not performed, 2nd stage simply inspects the invite and determines attestation level based on **simple rules/policy**
  - Trust is **initiated/maintained/non-existant** end-to-end within the network

# How to we enforce trust?  Bigger picture

- We can view the service provider network as a **microcosm** of the larger telephone network
- We go back to hop-by-hop nature of network, trust must be maintained
    - end-to-end
    - SP-to-SP
    - caller-to-callee
- This can obviously be extended to
    - country-to-country
    - jurisdiction-to-jurisdiction

By Jacob de Gheyn II - Wapenhandelinghe Van Roers. Mvsqvetten. Ende Spiessen., Public Domain

# Beyond the crypto and signatures

- In order to maintain end-to-end trust, it all starts with **not certificates**, **not tokens**, **not STIR/SHAKEN**, but
  - **Vetting**, both customer and associated identity(s) and RCD
  - Proper management of customer provisioning, **ideally at the source of truth**, the service systems that support the customer


By Charles Vernier (1831-1887) - http://www.affichezvous.fr/PBSCProduct.asp?ItmID=7583934, Public Domain

# What's next?

- **Spoofing** really needs to **go away**
- **We now have the tools** to accomplish what spoofing has enabled in the past in a **truthful/ trusted way**
- This is a **fundamental loophole** scammers take advantage of, we need to remove that ability
- Converging on **implementing end-to-end trust** is key
- **Spoofing is simply not a legitimate part of any secure application**
- In order to get there...