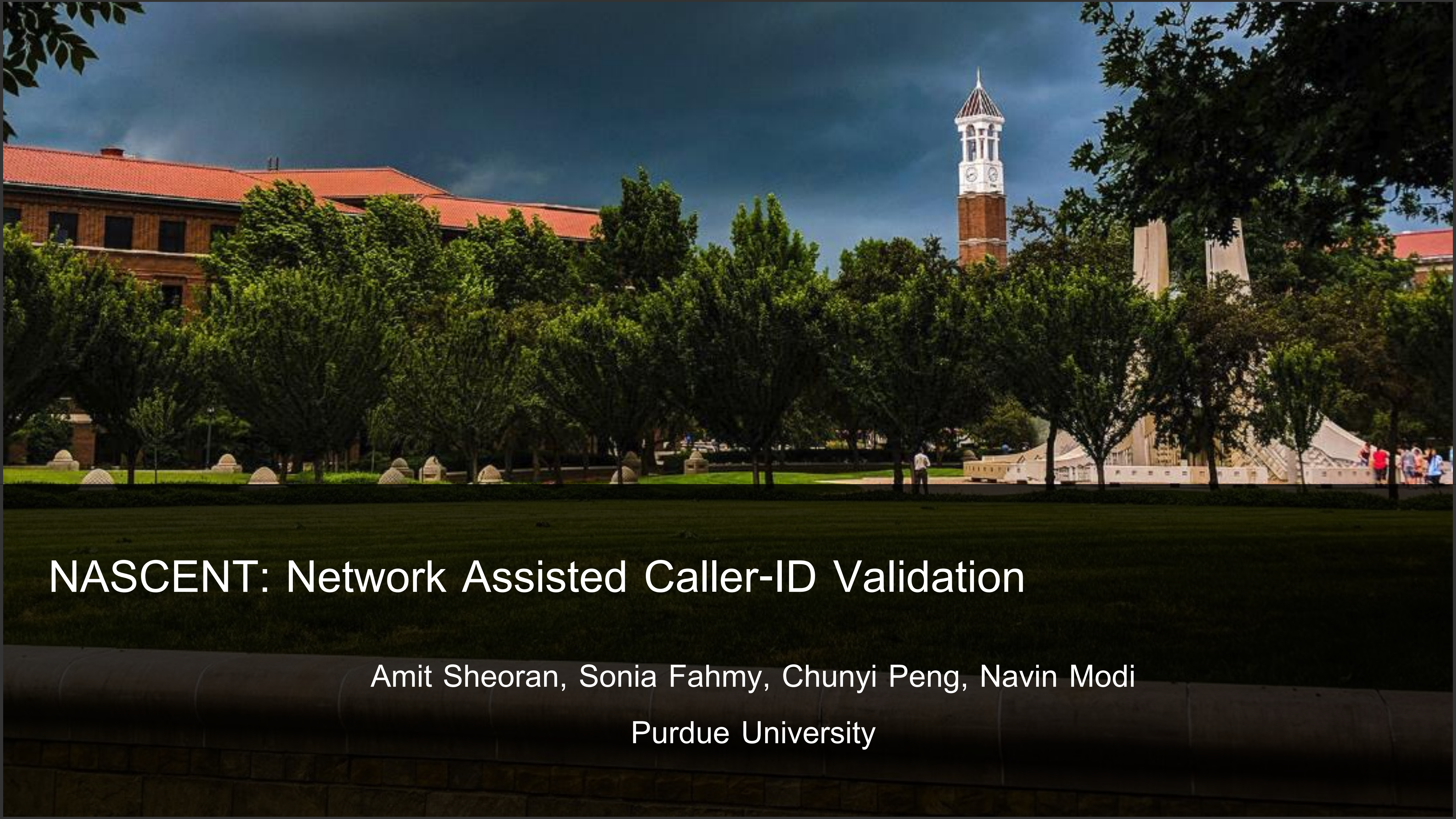


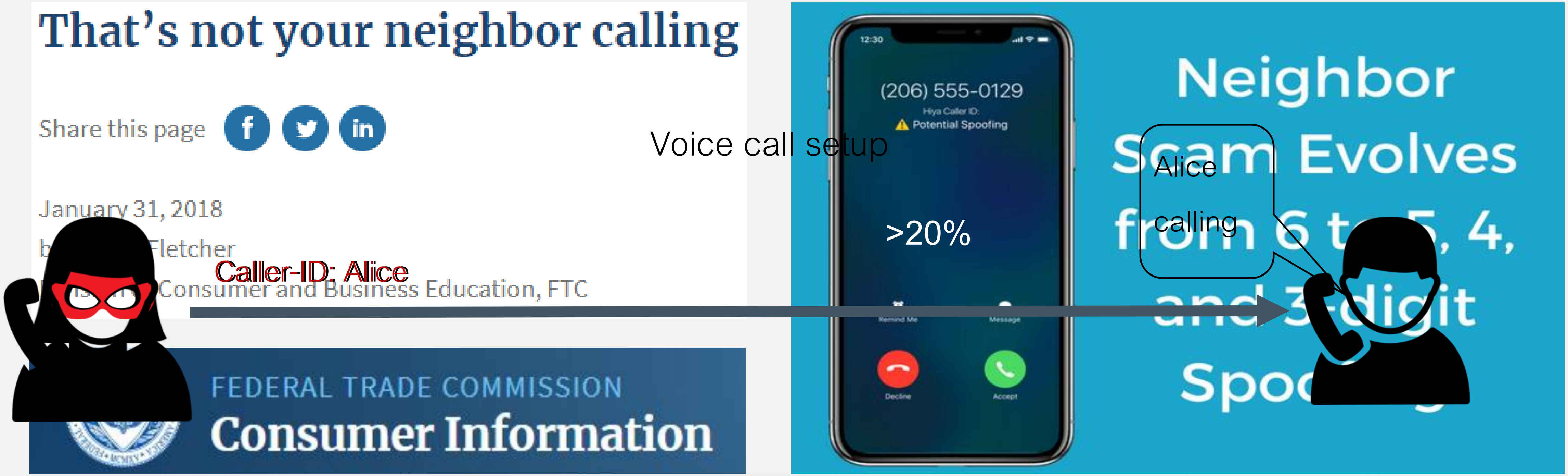
NASCENT: Network Assisted Caller-ID Validation

Amit Sheoran, Sonia Fahmy, Chunyi Peng, Navin Modi

Purdue University

What is caller-ID spoofing?

Caller deliberately falsifies their caller-ID to disguise their identify



That’s not your neighbor calling

Share this page

January 31, 2018

b Fletcher

Consumer and Business Education, FTC

FEDERAL TRADE COMMISSION

Consumer Information

12:30

(206) 555-0129

Hiya Caller ID:

Potential Spoofing

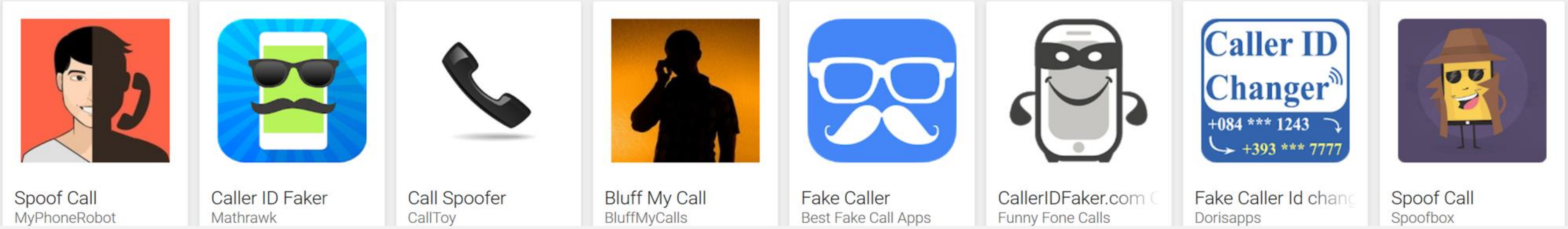
Remind Me

Message

Decline

Accept

Neighbor Scam Evolves from 6 t 5, 4, and 3-digit Spoo



Spoof Call
MyPhoneRobot

Caller ID Faker
Mathrawk

Call Spoofer
CallToy

Bluff My Call
BluffMyCalls

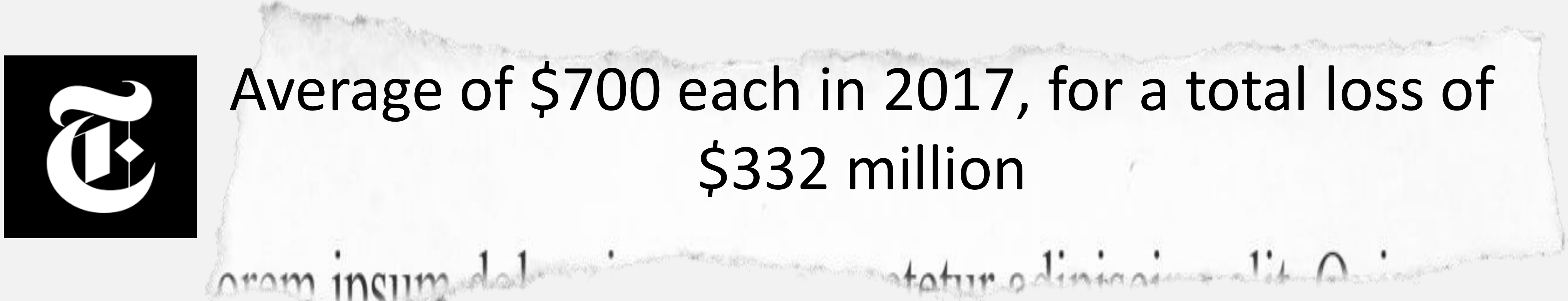
Fake Caller
Best Fake Call Apps

CallerIDFaker.com
Funny Fone Calls

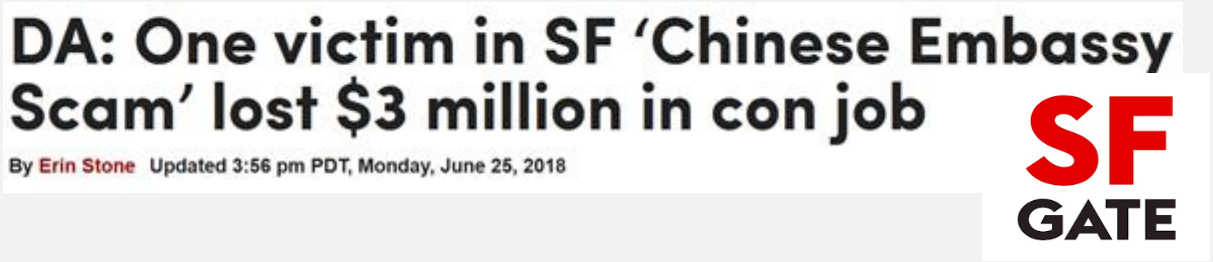
Fake Caller Id chan
Dorisapps

Spoof Call
Spoofbox

Why worry about caller-ID spoofing?

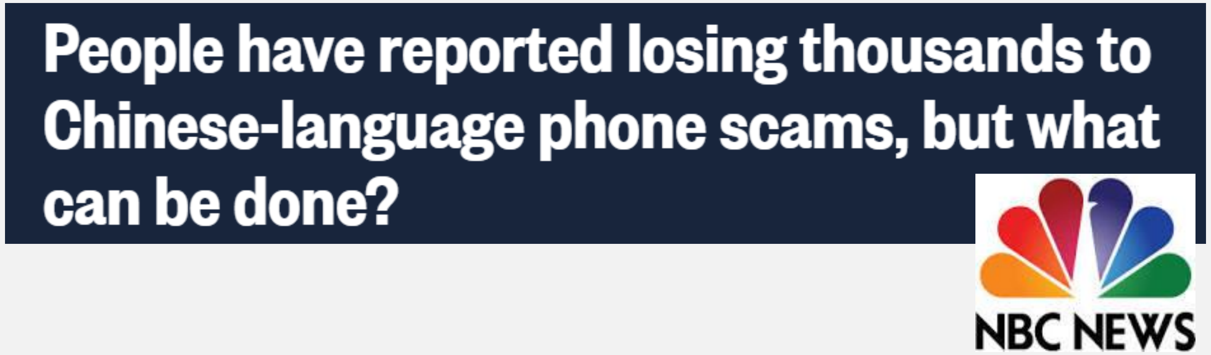


Average of $700 each in 2017, for a total loss of $332 million

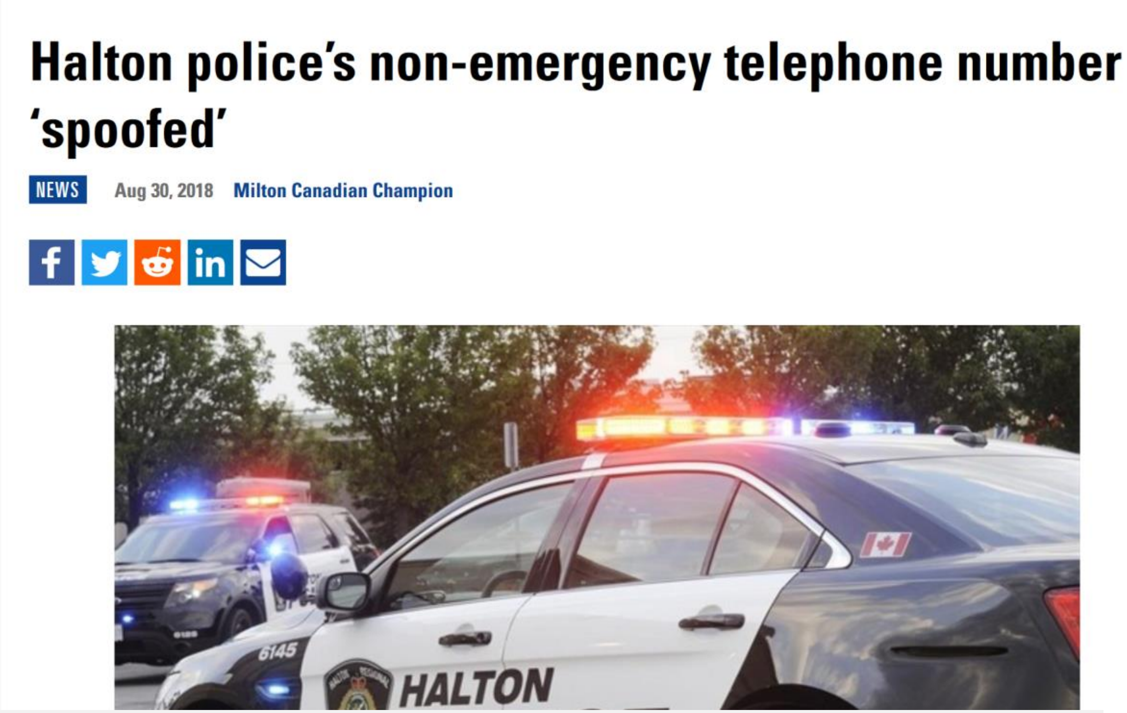


DA: One victim in SF 'Chinese Embassy Scam' lost $3 million in con job

By Erin Stone Updated 3:56 pm PDT, Monday, June 25, 2018



People have reported losing thousands to Chinese-language phone scams, but what can be done?

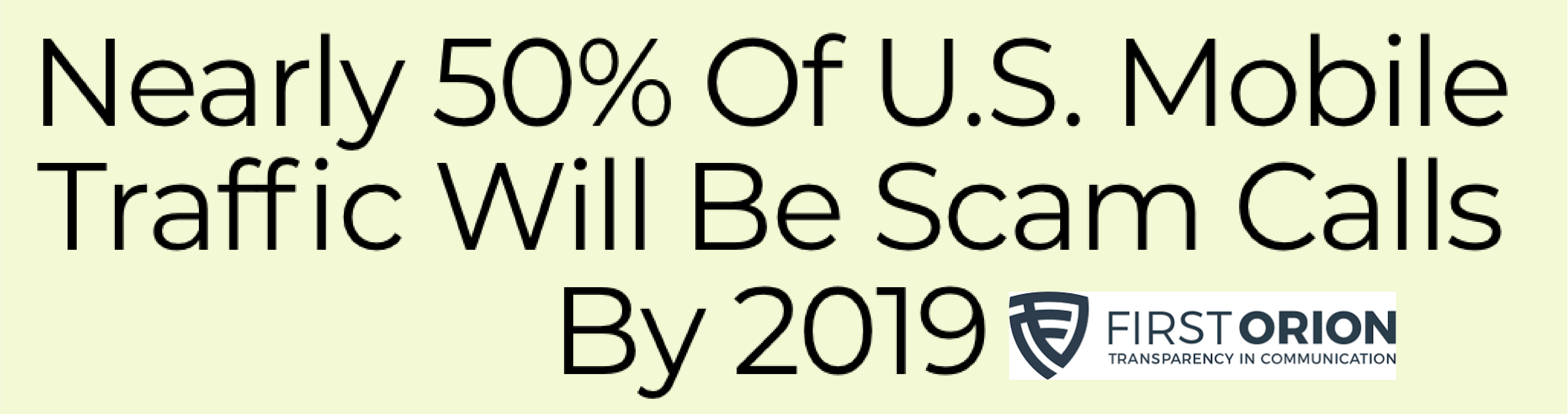


Halton police's non-emergency telephone number 'spoofed'

NEWS Aug 30, 2018 Milton Canadian Champion

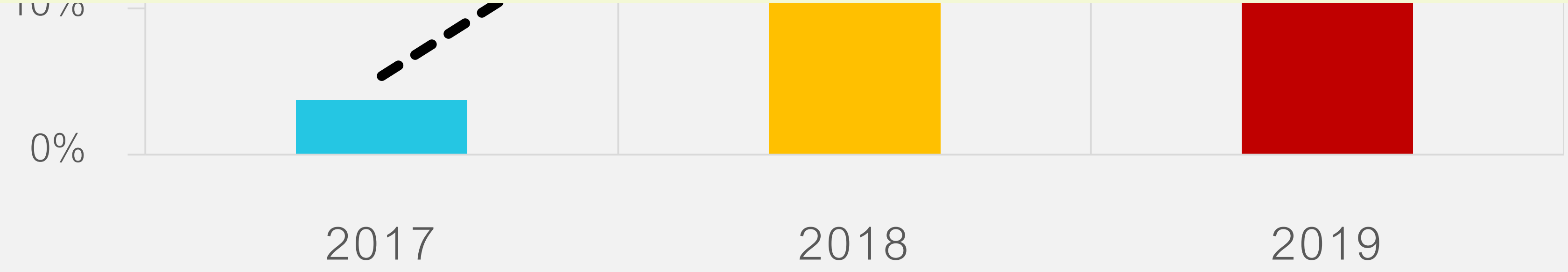
Caller-ID spoofing is a growing problem

% OF SPOOFED CALLS IN THE US

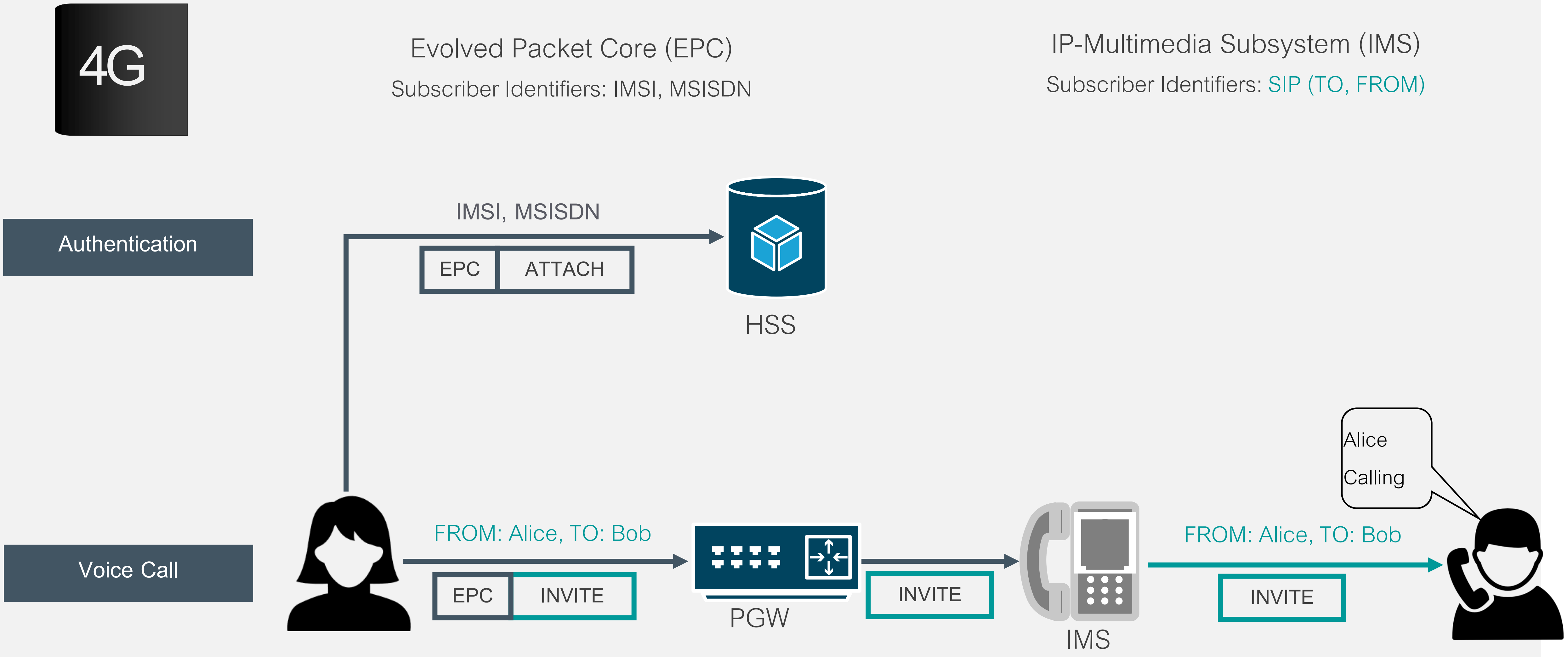


Nearly 50% Of U.S. Mobile Traffic Will Be Scam Calls By 2019

FIRST ORION
TRANSPARENCY IN COMMUNICATION



Why is caller-ID spoofing still feasible?



Lack of runtime authentication

4G

Evolved Packet Core (EPC)

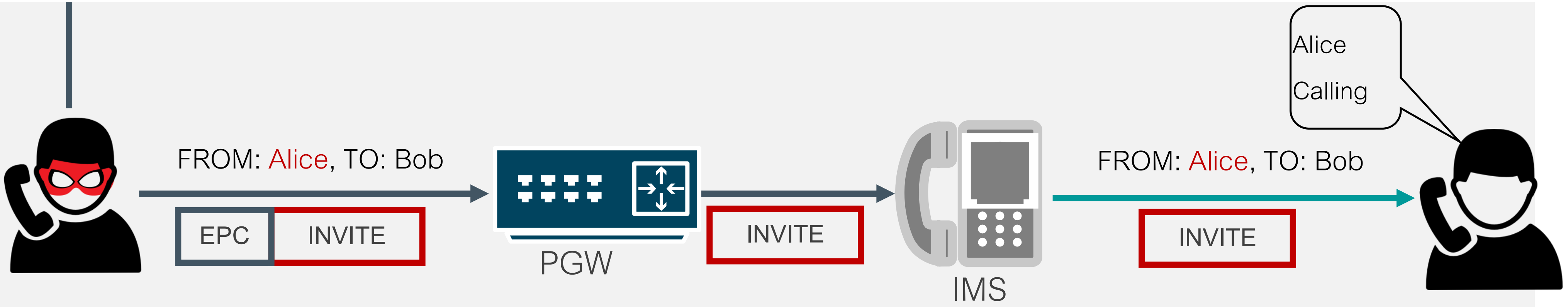
Subscriber Identifiers: IMSI, MSISDN

IP-Multimedia Subsystem (IMS)

Subscriber Identifiers: SIP (TO, FROM)

Lack of *Runtime Authentication* in VoLTE calls can lead *to caller-ID spoofing*

Voice Call



Existing solutions

Network

Passive Validation

Network

Active User Authentication (CHAP, TLS)

Endpoint

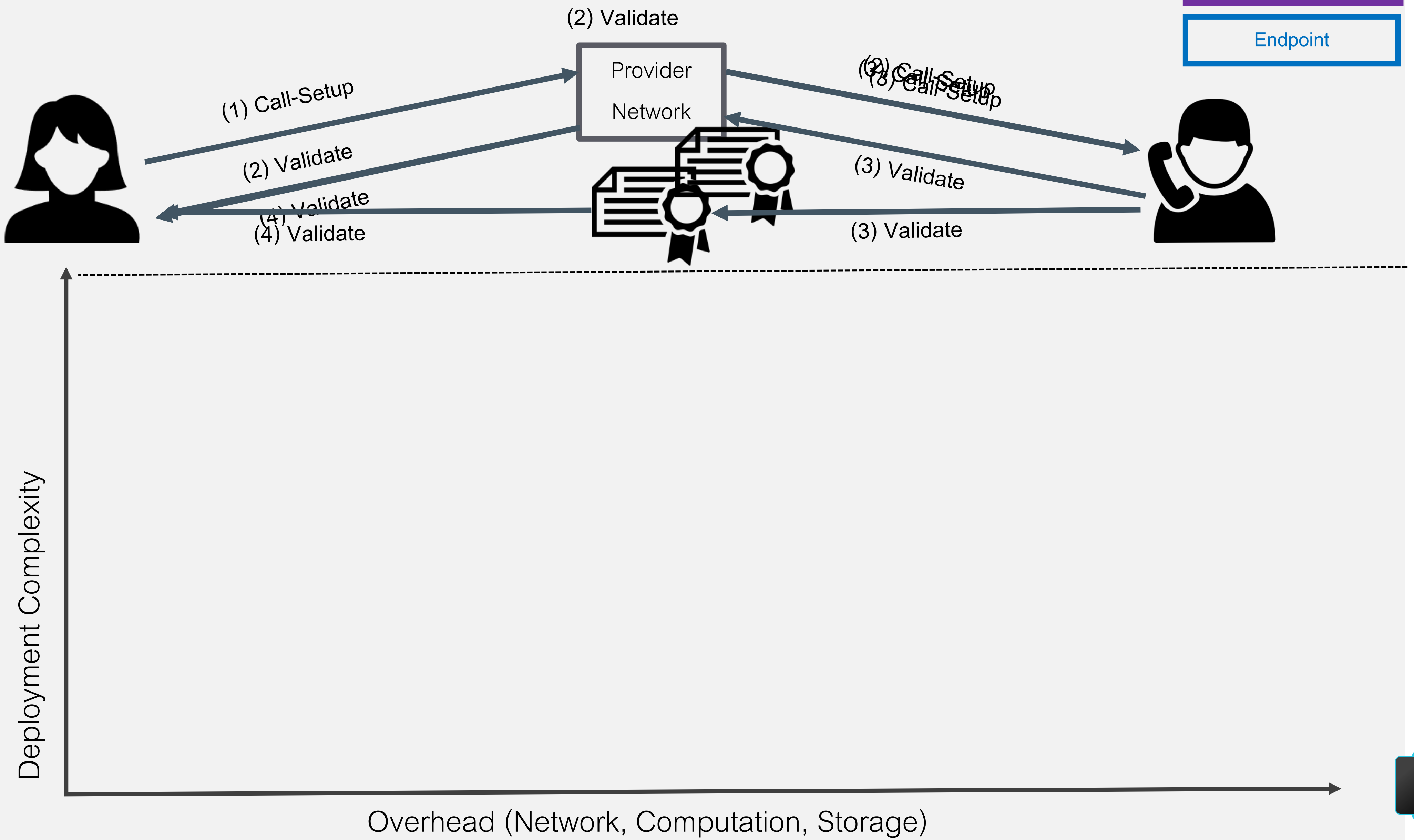
Callback Verification

Endpoint

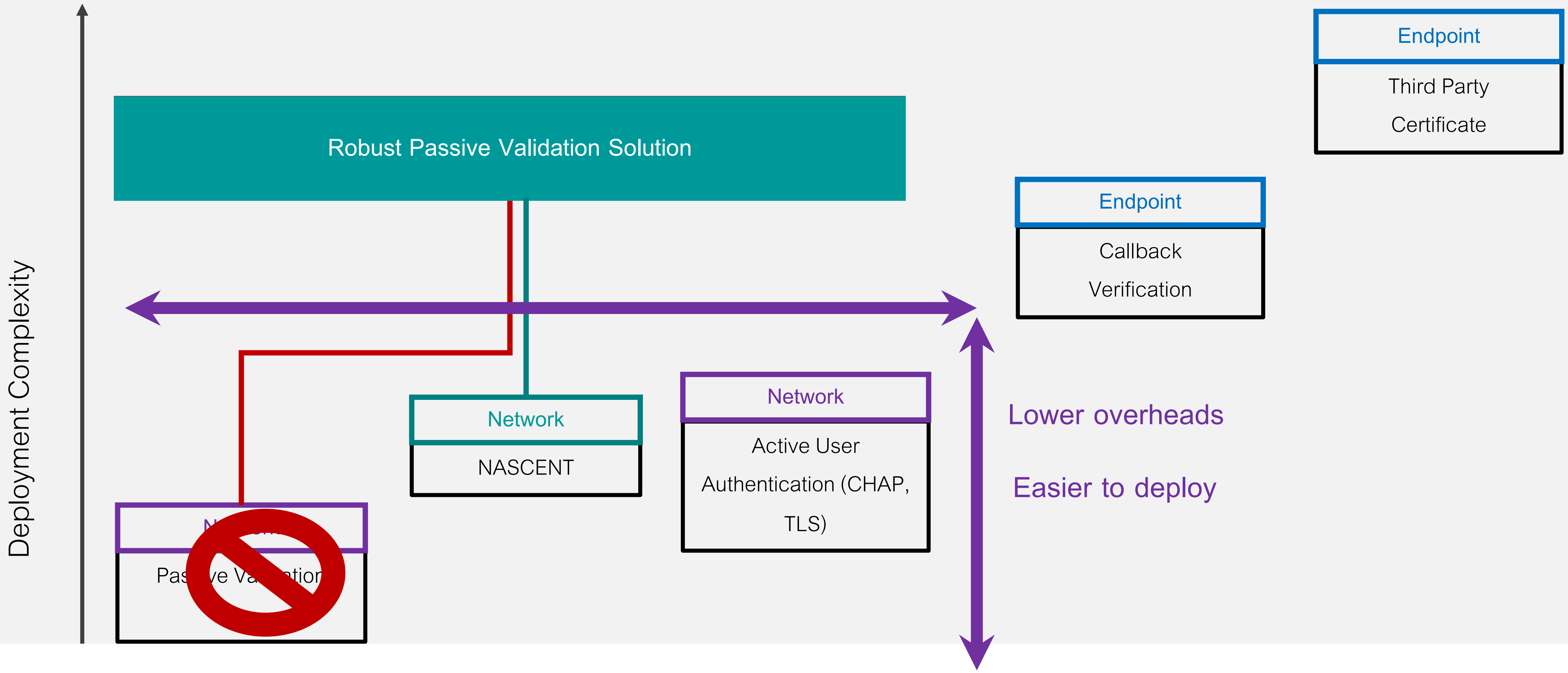
Third Party Certificate

Network

Endpoint



Comparison of runtime caller-ID validation solutions



Deployment Complexity

Robust Passive Validation Solution

Endpoint

Third Party Certificate

Endpoint

Callback Verification

Network

NASCENT

Network

Active User Authentication (CHAP, TLS)

Network

Passive Validation

Lower overheads

Easier to deploy

Telecom regulatory bodies such as the FCC in US now require network operators to provide caller-ID authentication

Network Assisted Caller-ID Validation with NASCENT

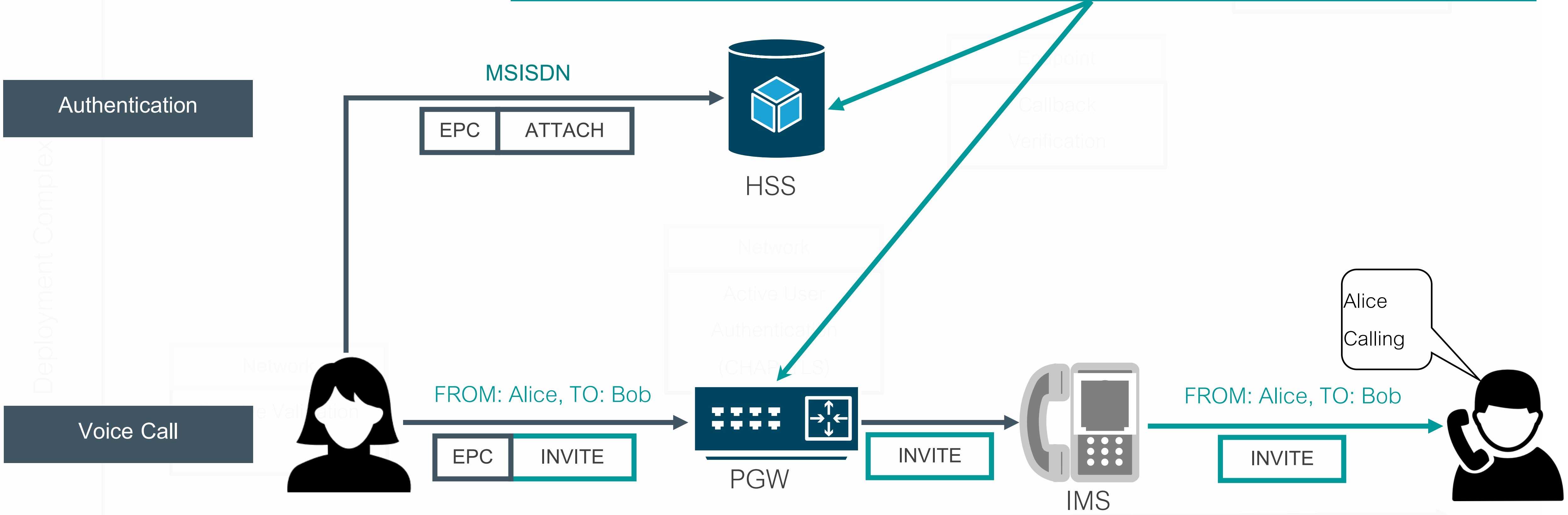
Detect

Analyze

Deploy

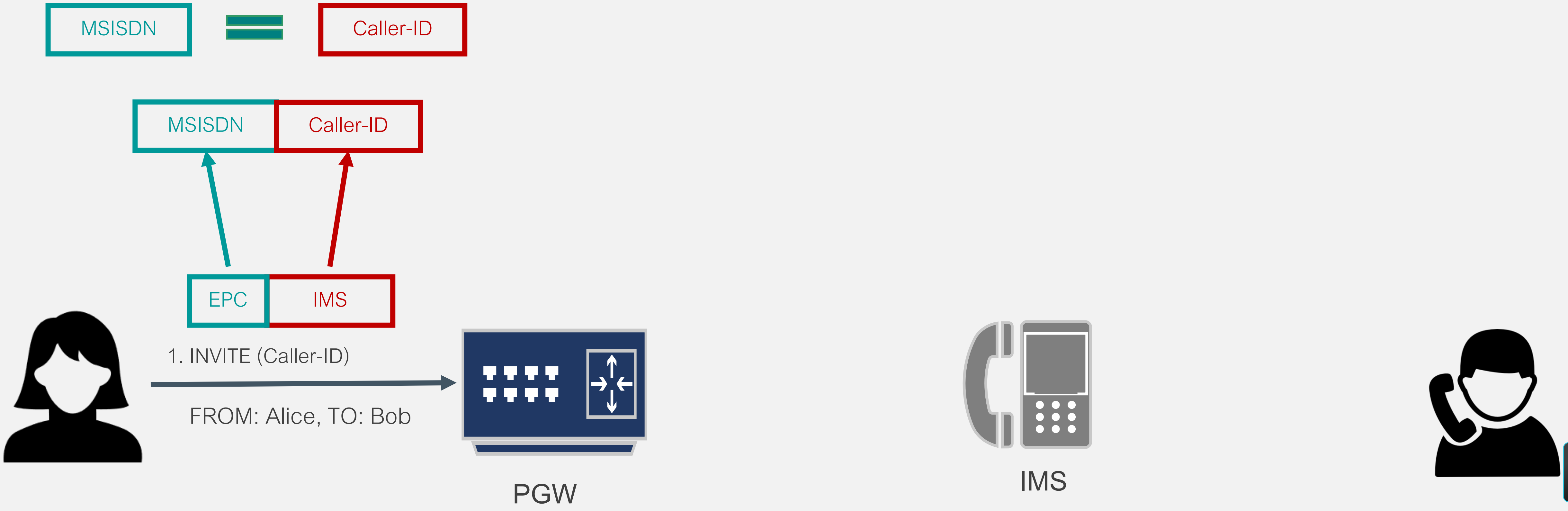
Why is caller-ID spoofing still feasible?

Can we leverage EPC authentication to support runtime caller-ID validation?



NASCENT - Key Idea

Leverage EPC authentication to perform runtime caller-ID validation

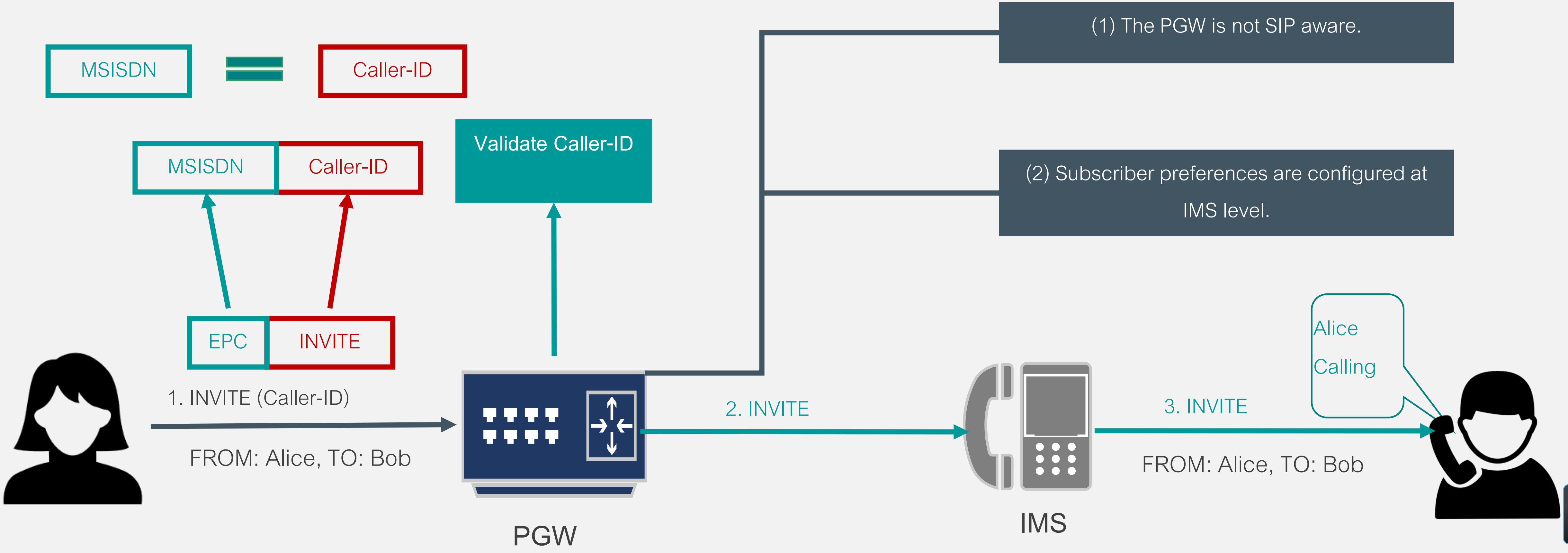


Detect

NASCENT - Key Idea

Detect

Leverage EPC authentication to perform runtime caller-ID validation

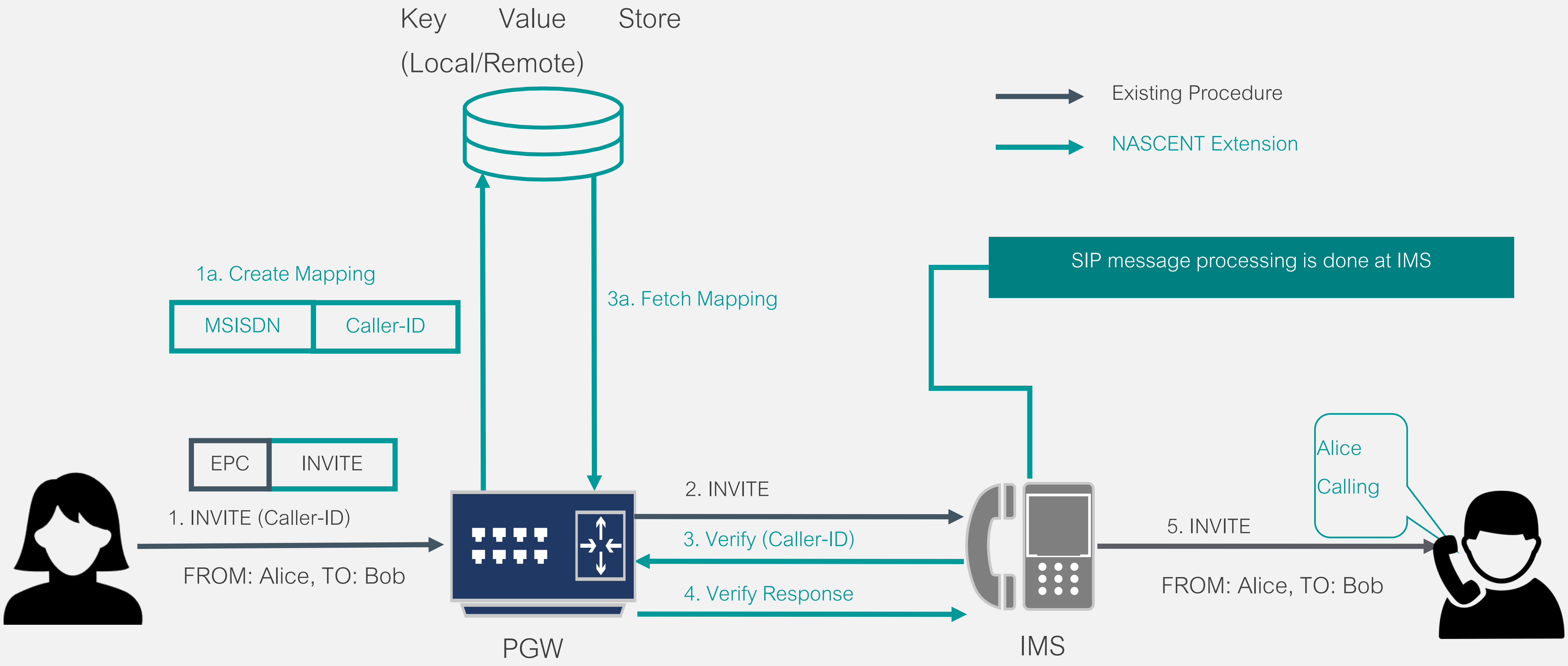


(1) The PGW is not SIP aware.

(2) Subscriber preferences are configured at IMS level.

Challenges in the real world (1)

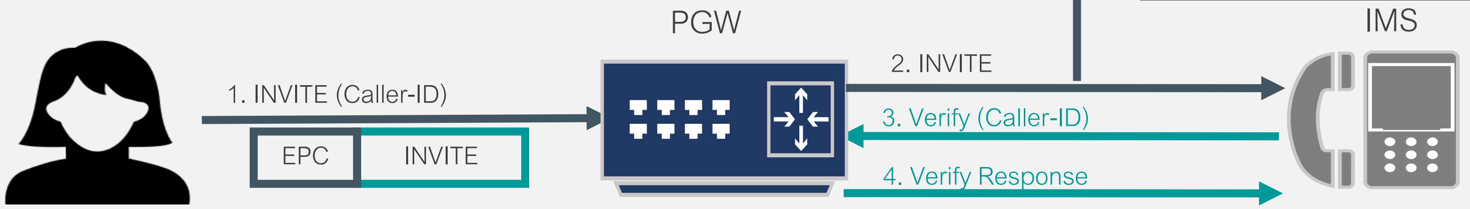
Leverage EPC authentication to perform runtime caller-ID validation



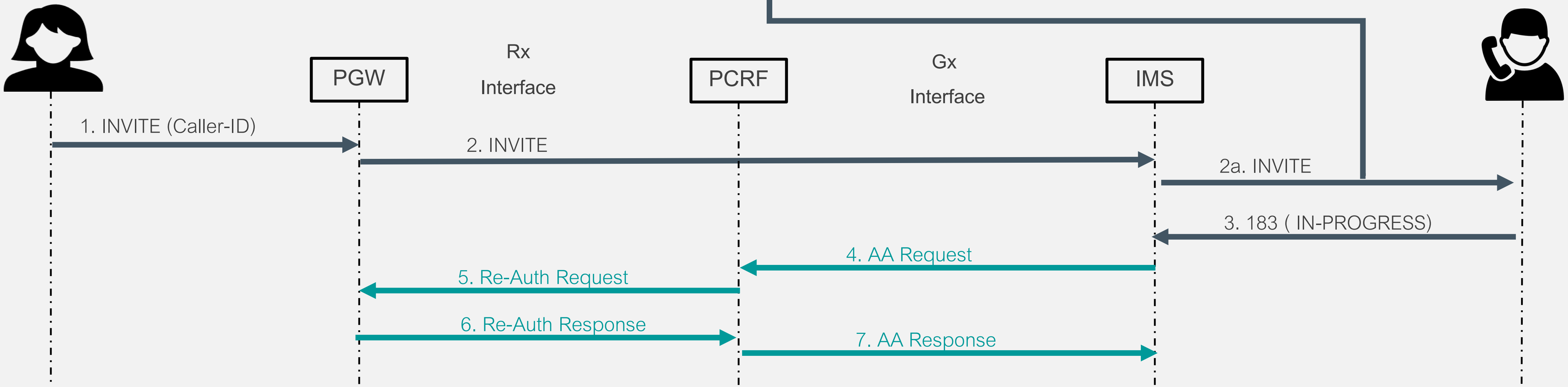
Challenges in the real world (2)

(1) No direct connection exists between the PGW and IMS

- PGW and IMS interface via the Policy Control and Charging Function (PCRF)

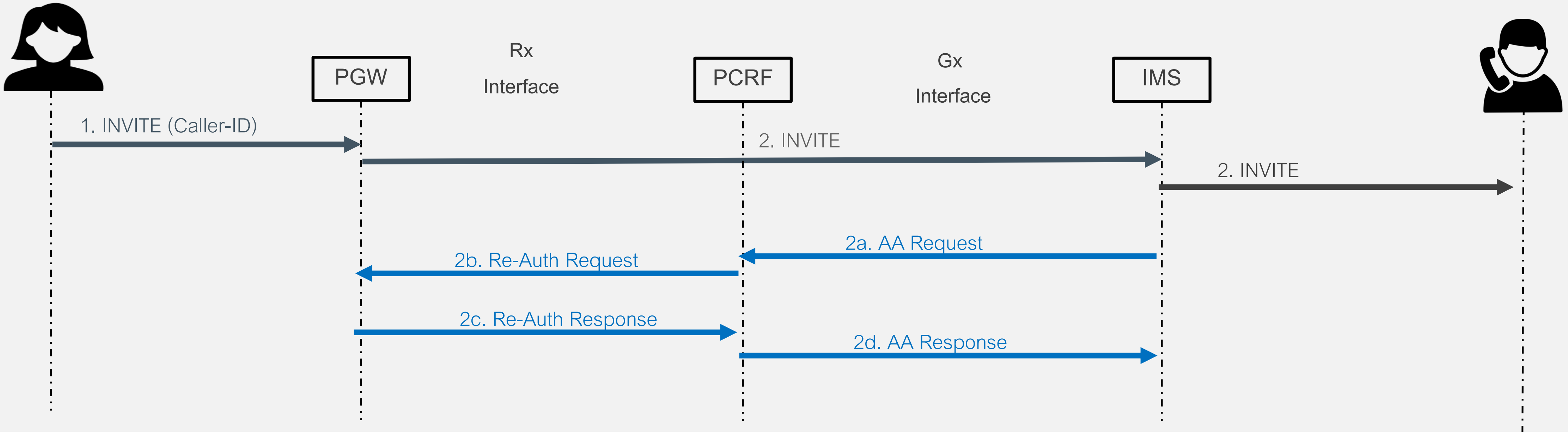


(2) IMS Access control procedure is performed after the Callee is Notified.



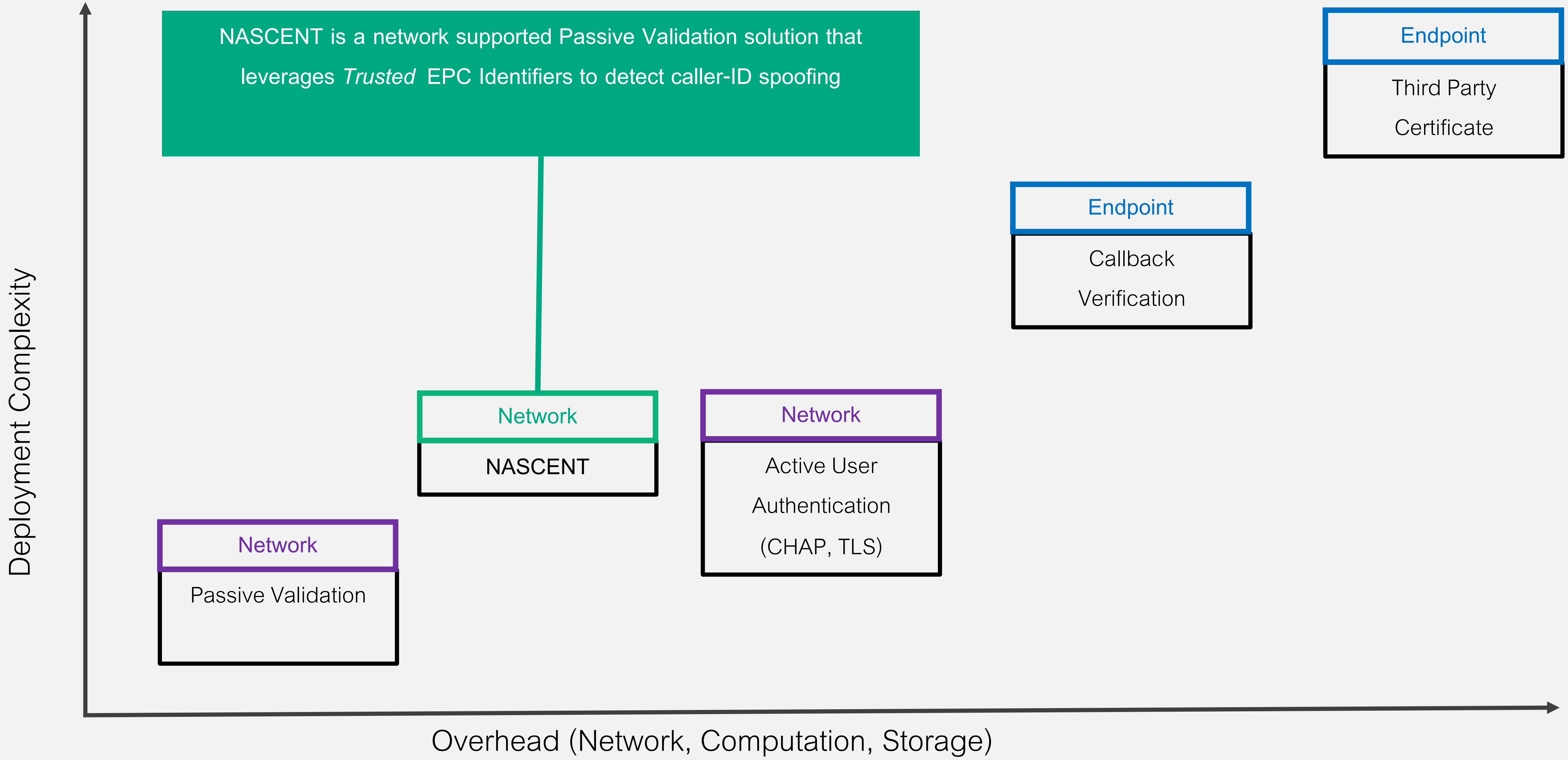
NASCENT: Trade-offs in the real world

Spoofed Call Notification	Overhead	Backward Compatibly	New Interfaces?	NASCENT Variant
Pre-Notification	Low	Yes	No	NASCENT-Rx-Gx



IMS Access control procedure is performed before the Callee is notified.

NASCENT vs Existing runtime caller-ID validation



NASCENT is a network supported Passive Validation solution that leverages *Trusted* EPC Identifiers to detect caller-ID spoofing

Experimental Evaluation

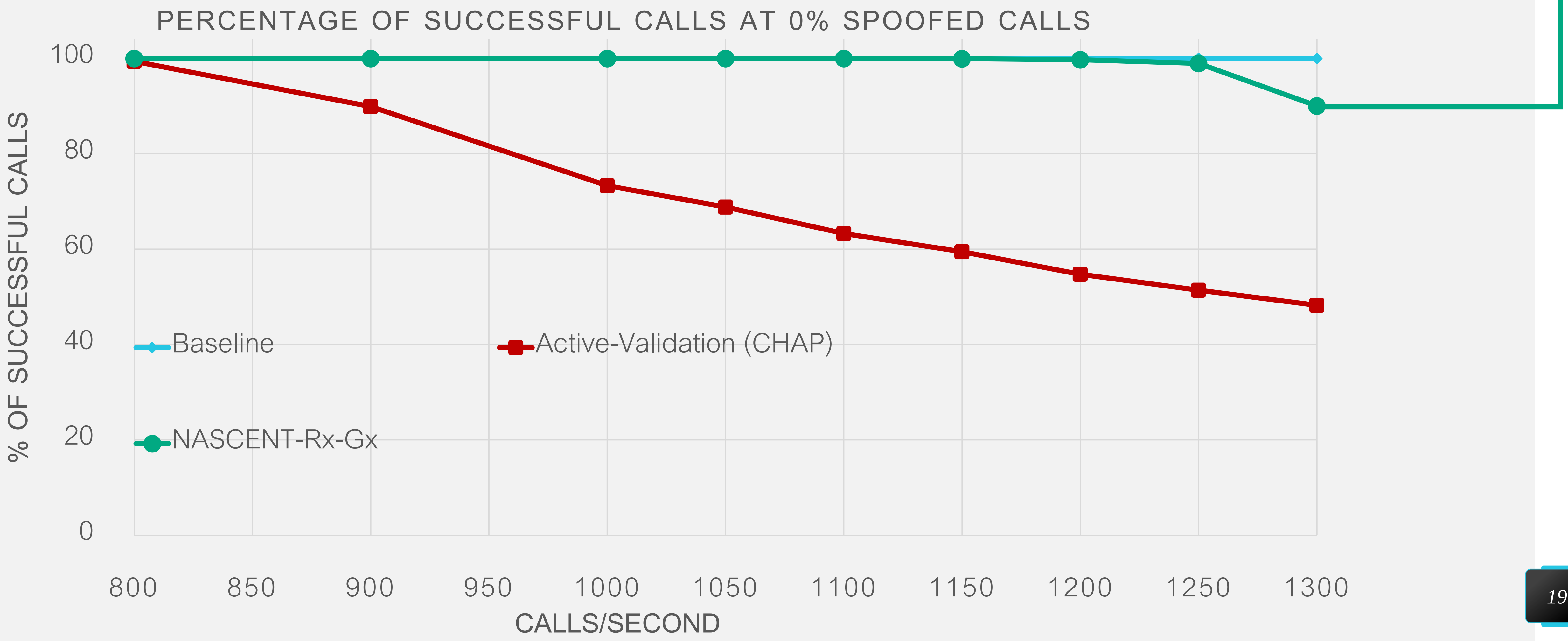
Experimental evaluation goals

Analyze

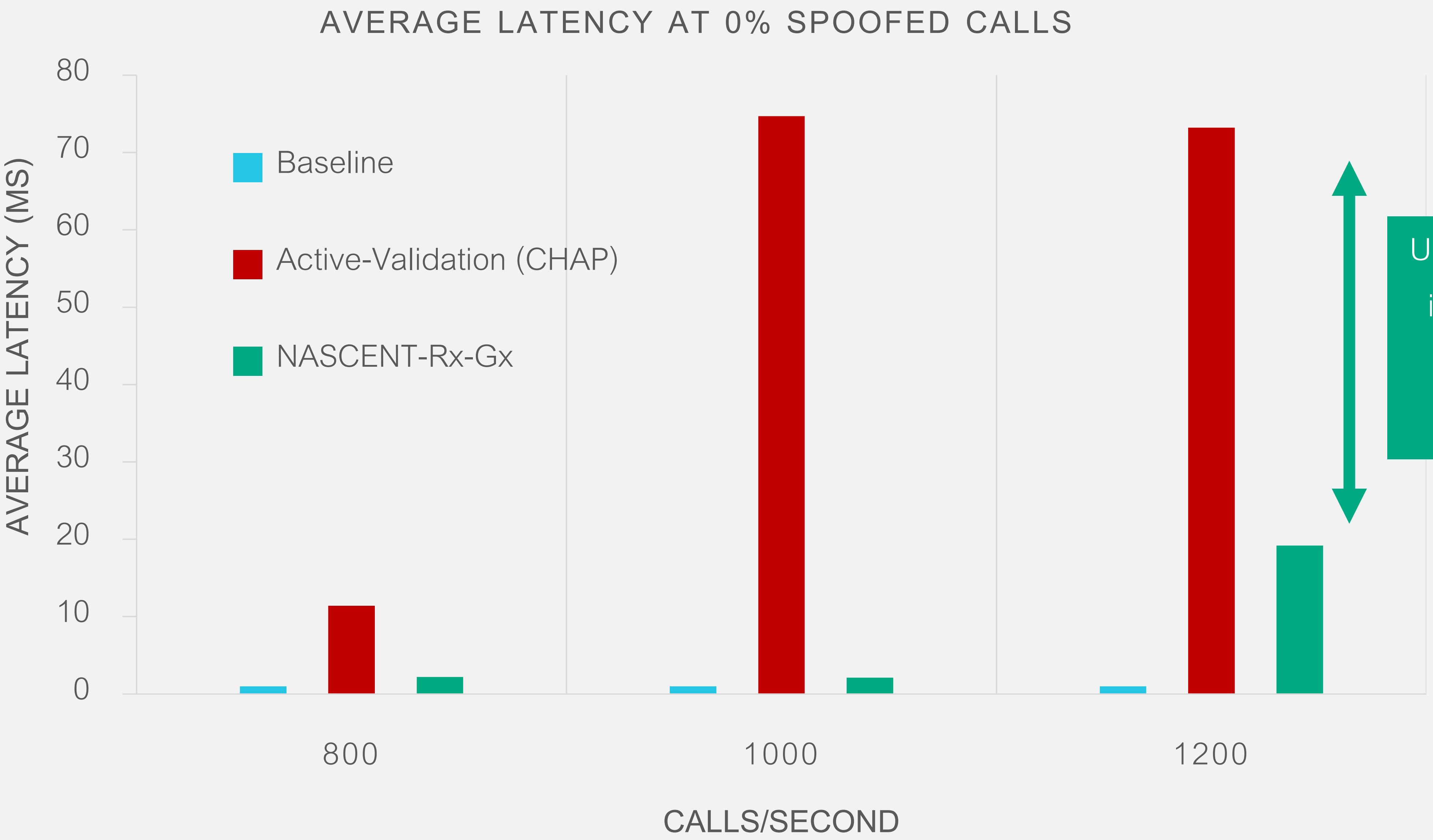
- What is the performance overhead of *NASCENT*?
  - Resource overhead (CPU)
  - Latency incurred by users
- How does *NASCENT* compare with other **Active User Authentication solutions** (CHAP)?

Evaluation results (Traditional Deployment)

NASCENT has significantly lower resource overhead



Evaluation results (Traditional Deployment)

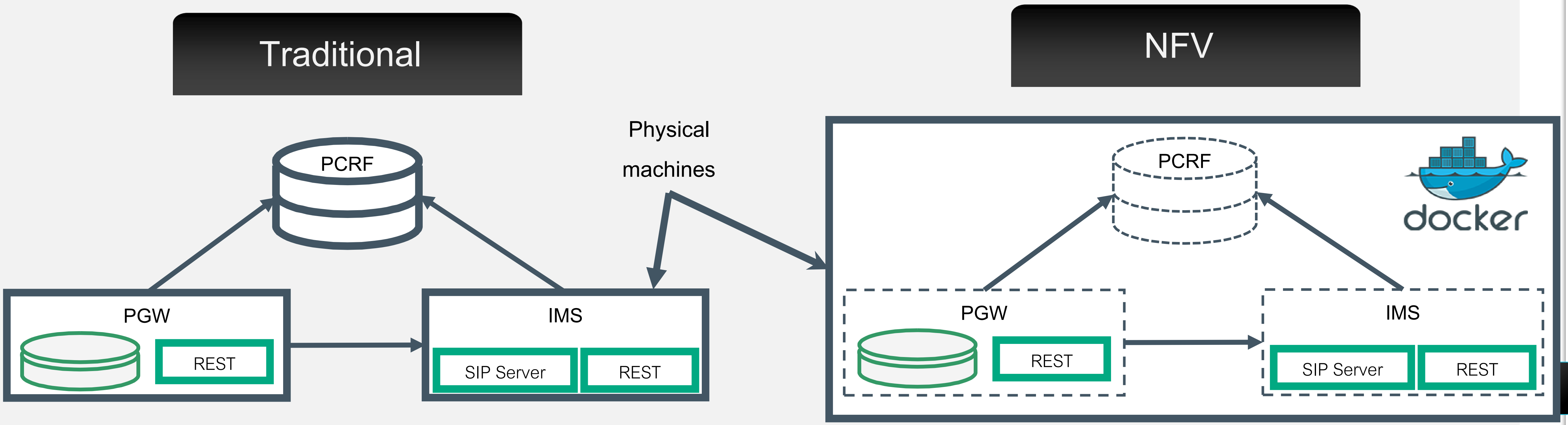


Up to 70% lower latency incurred compared to CHAP

Experimental evaluation goals

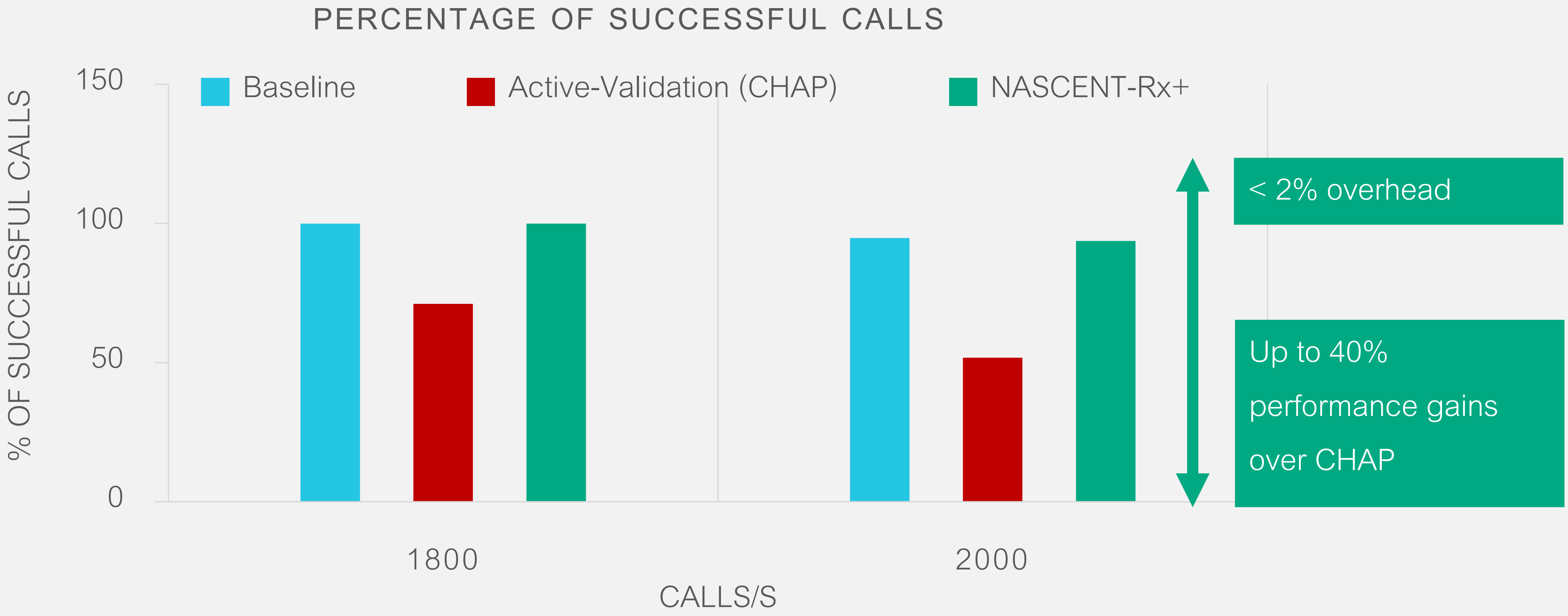
Deploy

- How does the Service Deployment Model impact the performance?



Evaluation results (NFV Deployment)

- Lower overheads due resource sharing between EPC and IMS



< 2% overhead

Up to 40% performance gains over CHAP

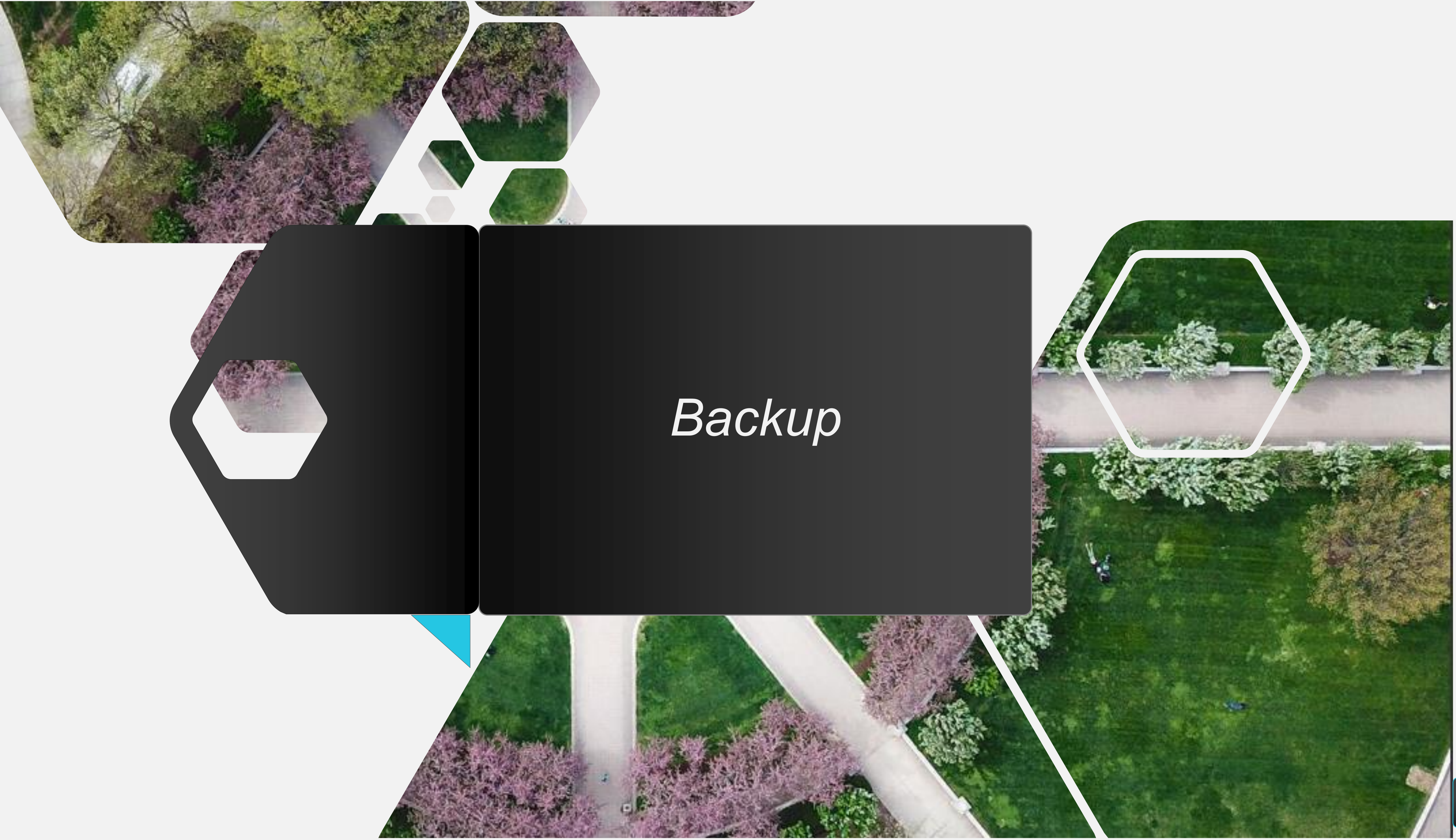
Much more in the paper..

- *NASCENT* variants and trade-offs
  - Backward compatibility vs performance overhead
- Selective validation of caller-ID
  - *NASCENT* has negligible overhead if 5% of calls are validated
- Will *NASCENT* work in 5G?

Conclusions

- Caller-ID spoofing is an important and challenging problem
  - Existing solutions have high infrastructure and performance overheads
- *NASCENT* proposes a cross validation based solution to detect Caller-ID spoofing
  - Leverage existing EPC authentication
  - Multiple variants to balance trade-offs
- *NASCENT* outperforms existing solutions

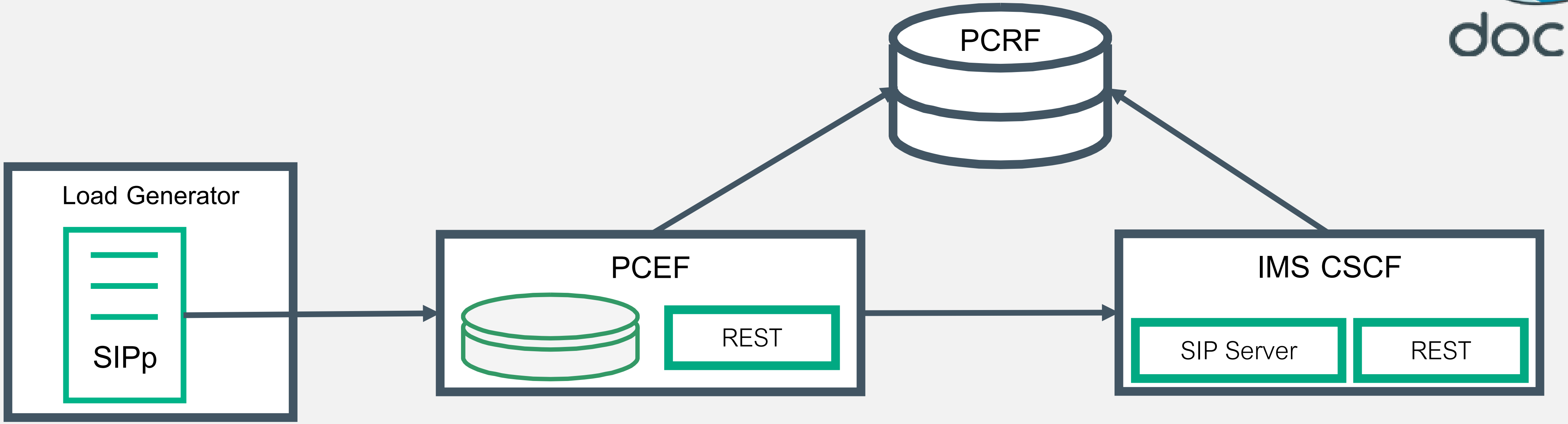
Questions?



Backup

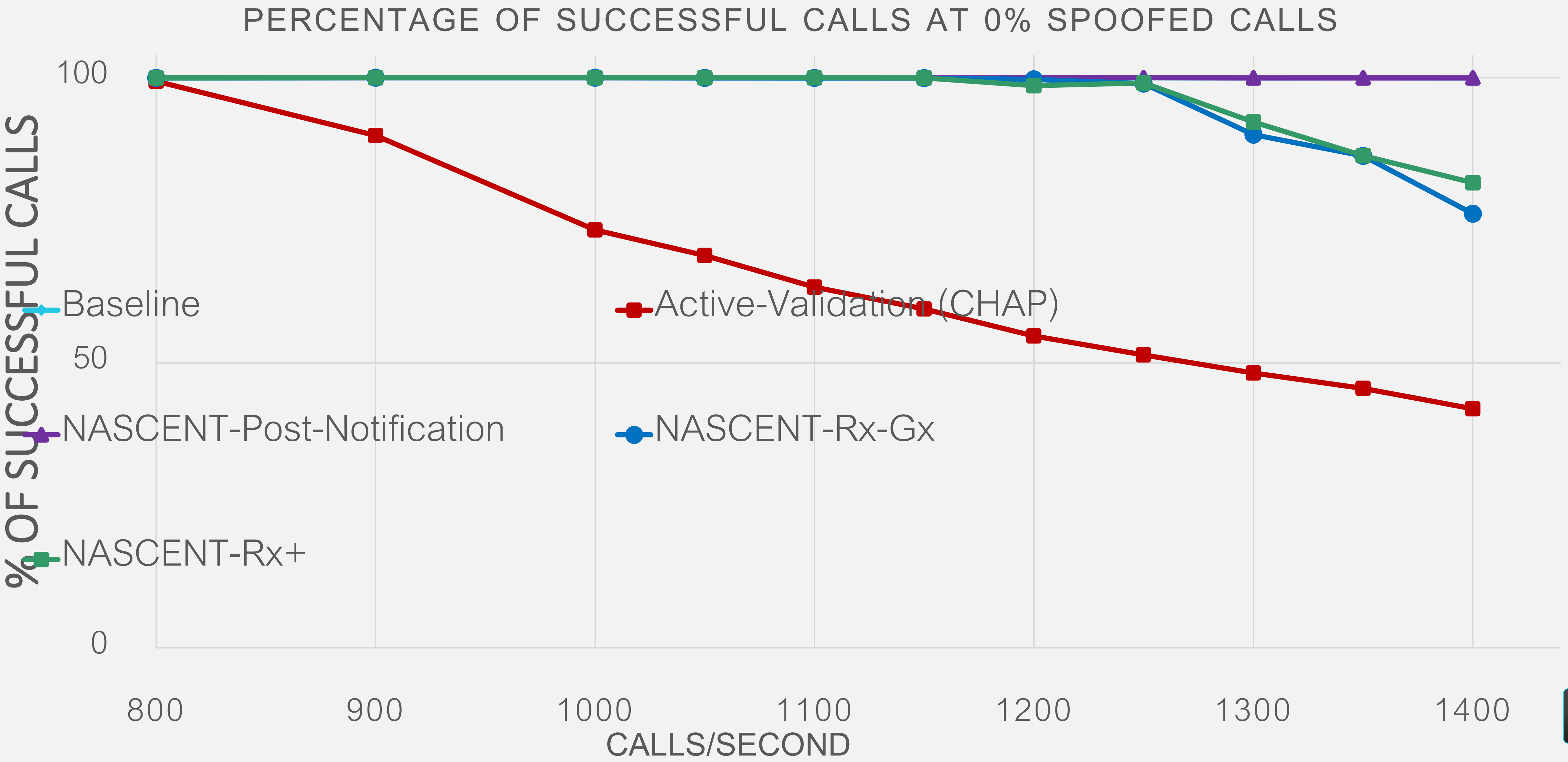
Experimental setup

docker

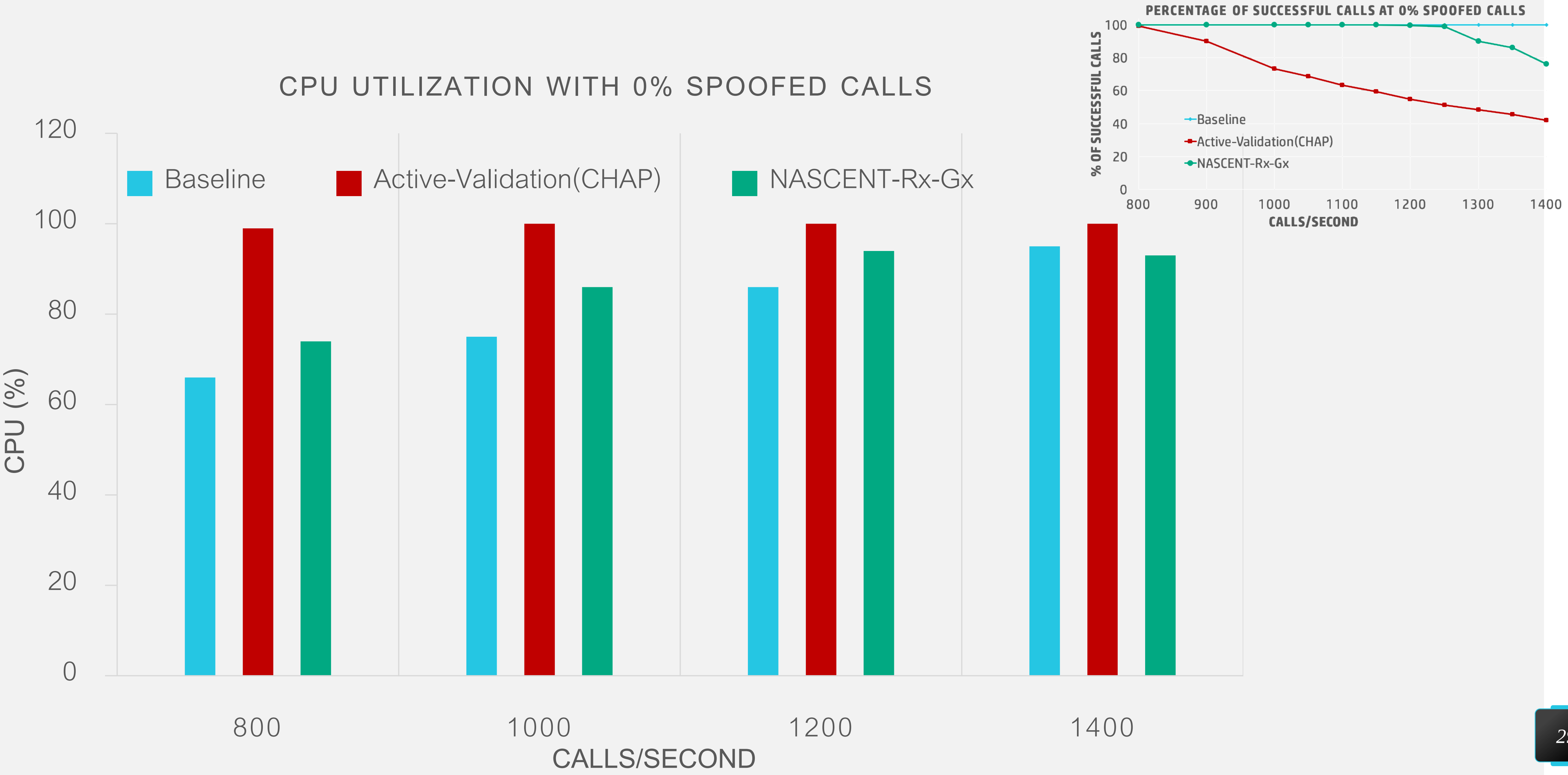


VNF	Functionality	Components	Software
IMS CSCF	SIP Call setup + Caller-ID validation	SIP Server + REST	KAMAILIO
PCEF	Tunnel SIP Traffic + Diameter Gx + Caller-ID Mapping management	REST, Diameter	KORE
PCRF	Diameter Gx + Rx Interface Support	Diameter	freeDiameter Diameter open implementation
Load Generator	Generate SIP traffic	SIPp	SIPp

Evaluation Results (Traditional Deployment)



Evaluation Results (Traditional Deployment)



Why is Caller-ID spoofing possible in 4G?

2G

Packet Delivery

+ Call AddressingCall Addressing

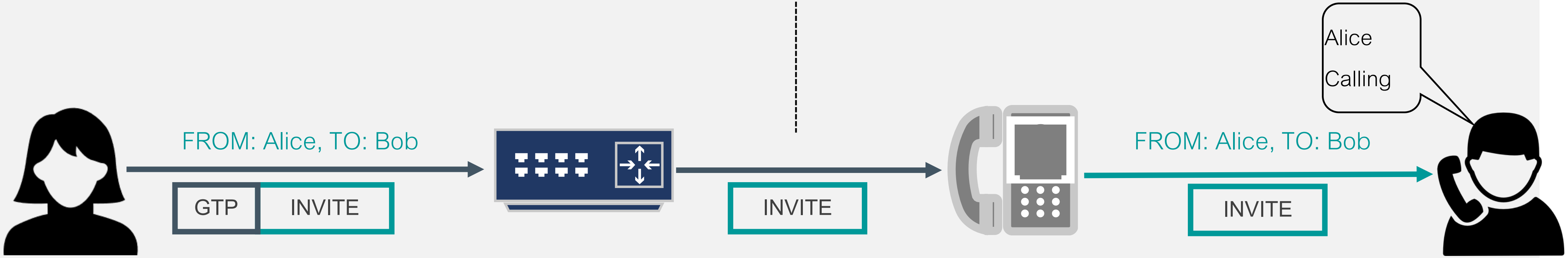
4G

Evolved Packet Core (EPC)

Subscriber Identifiers: IMSI, MSISDN

IP-Multimedia Subsystem (IMS)

Subscriber Identifiers: SIP (TO, FROM, etc)


Alice
Calling
FROM: Alice, TO: Bob
GTP
INVITE
INVITE
FROM: Alice, TO: Bob
INVITE