



ITU Kaleidoscope 2016
ICTs for a Sustainable World

**TOWARD AUTHENTICATED CALLER ID
TRANSMISSION: THE NEED FOR A STANDARDIZED
AUTHENTICATION SCHEME IN Q.731.3 CALLING
LINE IDENTIFICATION PRESENTATION**

**Huahong Tu, Adam Doupé, Ziming Zhao,
and Gail-Joon Ahn**

Arizona State University
tu@asu.edu

Bangkok, Thailand
14-16 November 2016


Americans lost \$8.6 billion to phone fraud in last year, survey suggests

Herb Weisbaum
TODAY

Aug. 27, 2014 at 10:25 AM

Survey: 11% of adults lost money to a phone scam last year

Millennials were one of the most victimized groups

01/26/2016 | ConsumerAffairs |  Scams

The New York Times | <http://nyti.ms/ZBKHRz>

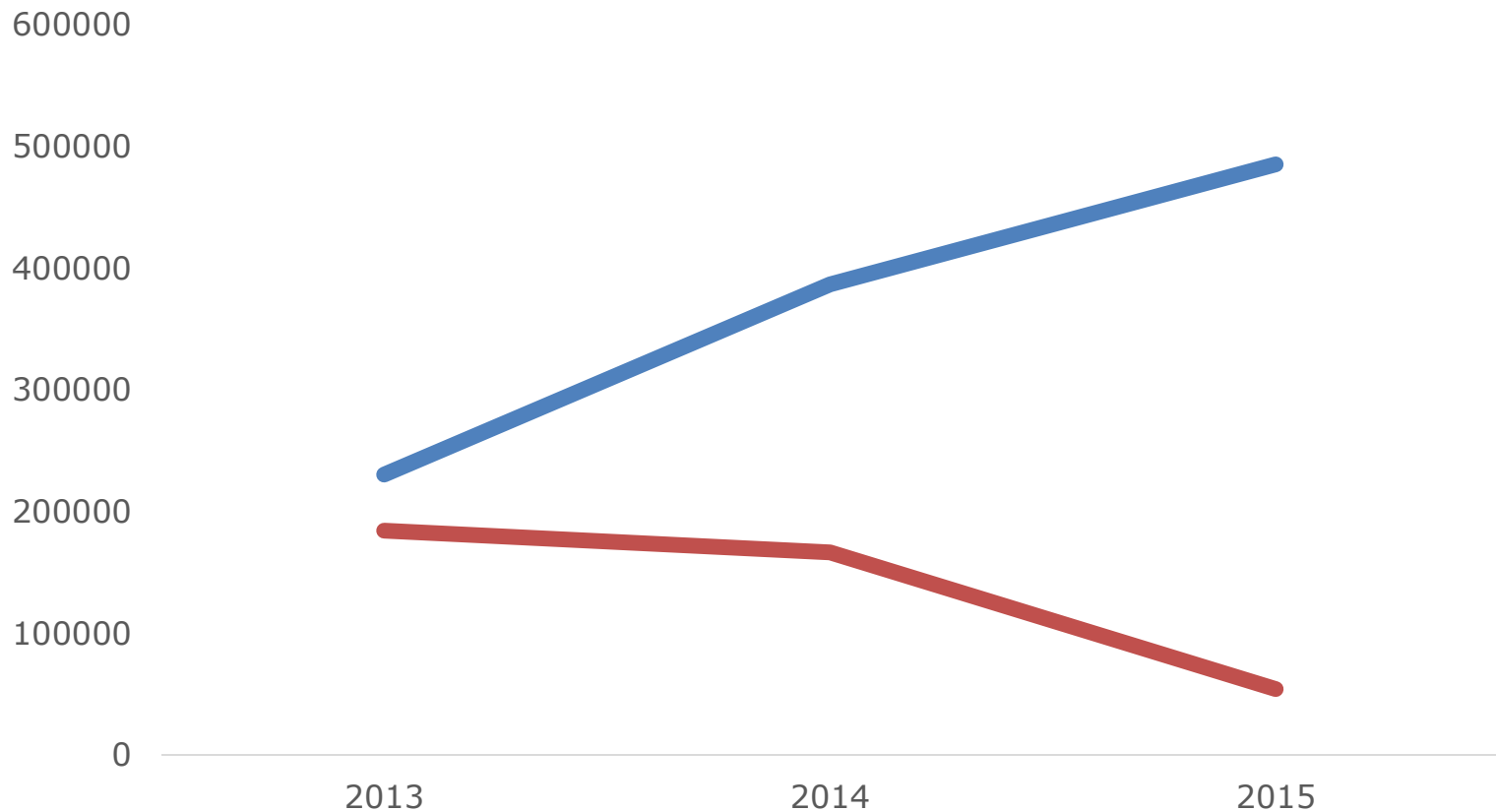
TECHNOLOGY

Phone Hackers Dial and Redial to Steal Billions

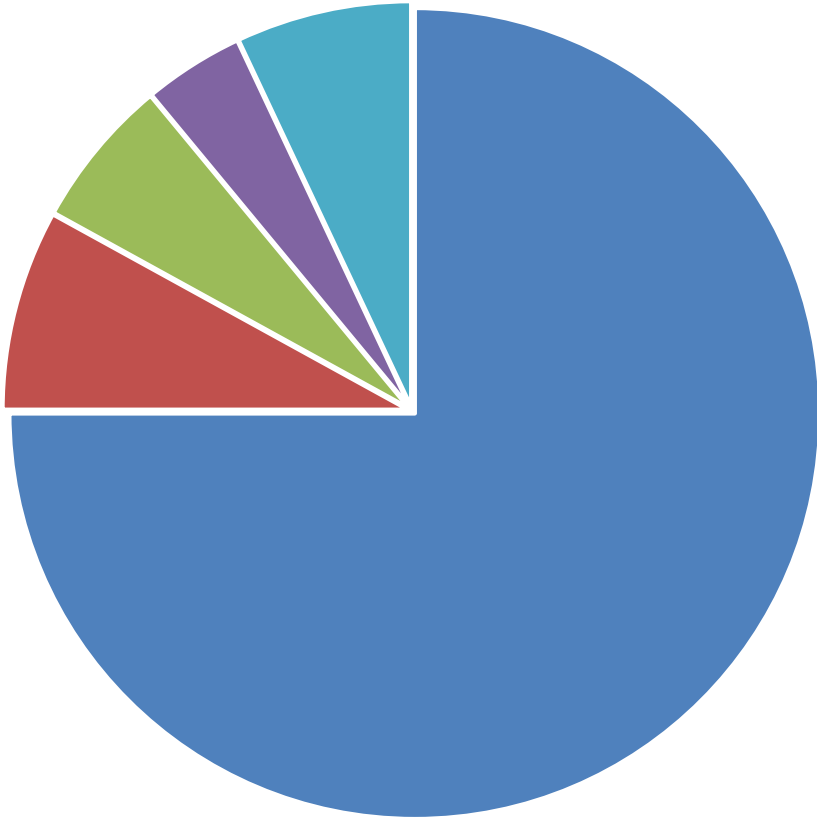
By NICOLE PERLROTH OCT. 19, 2014

Fraud Complaints by Method of Contact 2013-2015

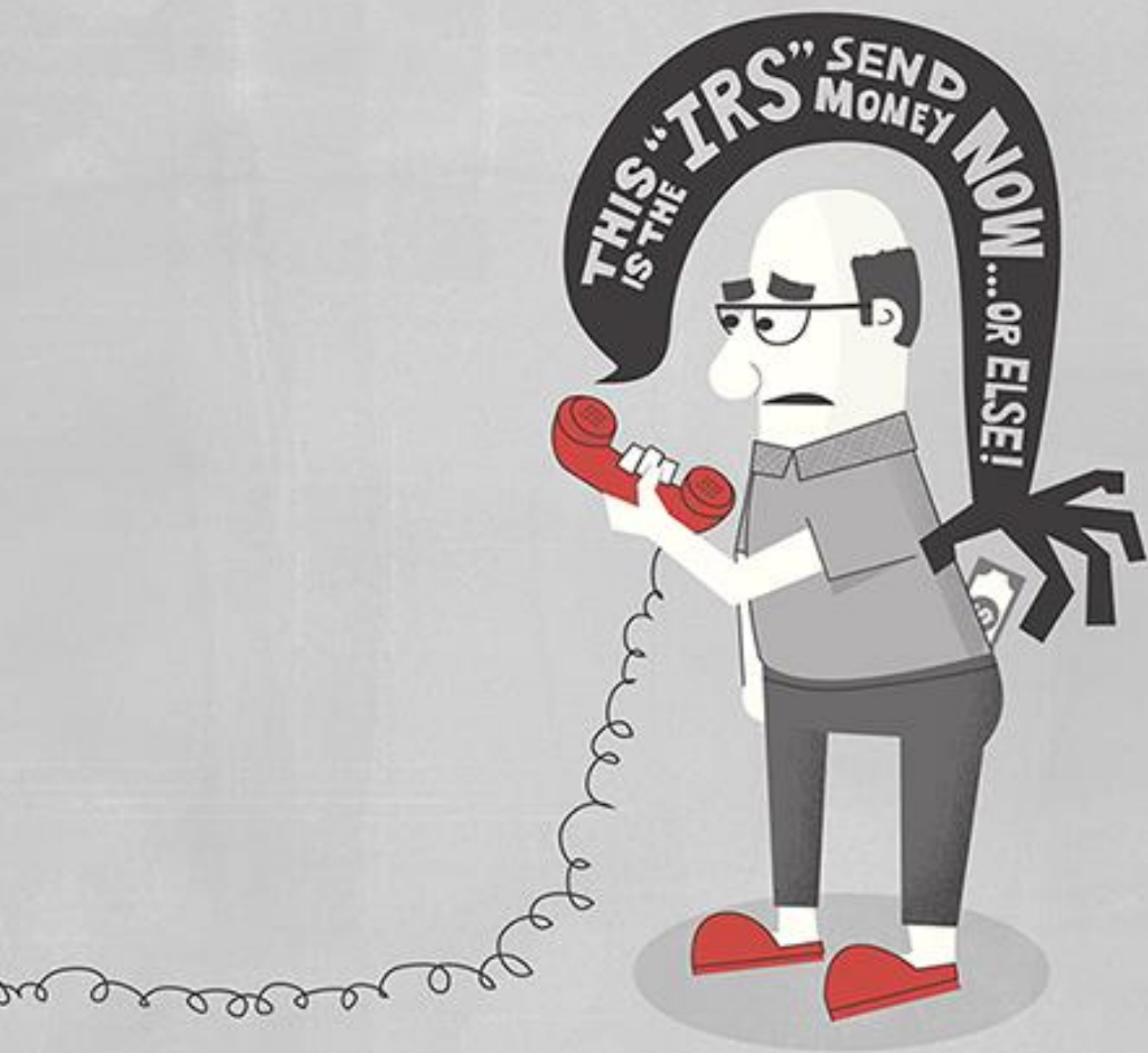
— Phone — Email



Fraud Complaints by Method of Communication in 2015



■ **Phone** ■ Email ■ Web ■ Mail ■ Other







Call Blocker



012679467643

Block call



01256734976

Block call



01256793467

Block call



01697546764

Block call



01646767643

Block call



01675467646

Block call



01276467643

Block call



01234676437

Block call



01256634676





**NATIONAL
DO NOT CALL
REGISTRY**



OC Watchdog

Fed up with rising robocalls, millions say 'Do Not Call' list doesn't work and want relief

Oct. 3, 2016 | *Updated Oct. 5, 2016 7:13 a.m.*





Step 1: What type of broadcast would you like to create?

Message Type Voice Only

Text Only

Voice & Text

Name this Broadcast

Caller ID

Broadcast Type Announcement [?]

Survey [?]

Next

Step 2: Who would you like to receive this message?

Step 3: When would you like your broadcast to start?

Step 4: What is your voice message?

Step 5: Review and Submit

Recommendation Q.731

STAGE 3 DESCRIPTION FOR NUMBER IDENTIFICATION SUPPLEMENTARY SERVICES USING SIGNALLING SYSTEM No. 7

	8	7	6	5	4	3	2	1
1	O/E	Nature of address indicator						
2	NI	Numbering plan indicator			Address presentation restricted indicator		Screening indicator	
3	2nd address signal				1st address signal			
:								
:								
m	Filler (if necessary)				<i>n</i> th address signal			

Figure 11/Q.763 – Calling party number parameter field

Recommendation Q.731

STAGE 3 DESCRIPTION FOR NUMBER IDENTIFICATION SUPPLEMENTARY SERVICES USING SIGNALLING SYSTEM No. 7

	8	7	6	5	4	3	2	1
1	O/E	Nature of address indicator						
2	NI	Numbering plan indicator			Address presentation restricted indicator		Screening indicator	
3	2nd address signal				1st address signal			
:	Spoo							
:								
m	Filler (if necessary)				<i>n</i> th address signal			

Figure 11/Q.763 – Calling party number parameter field


Why Security Indicators Matter



PayPal, Inc. [US]

<https://www.paypal.com/home>

   PayPal Inbox Updates Purchases We're transferring money to your bank

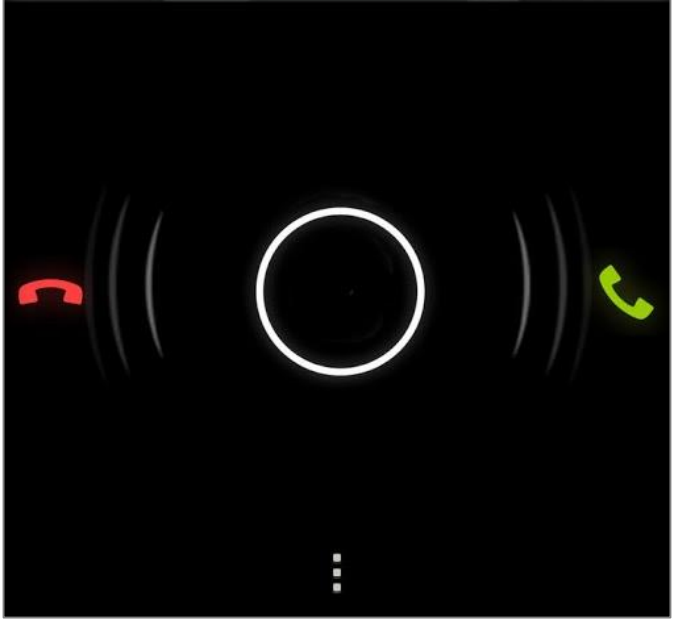
   PayPal Inbox Updates Purchases You sent a payment



 PayPal

1 (402) 935-2050

INCOMING CALL



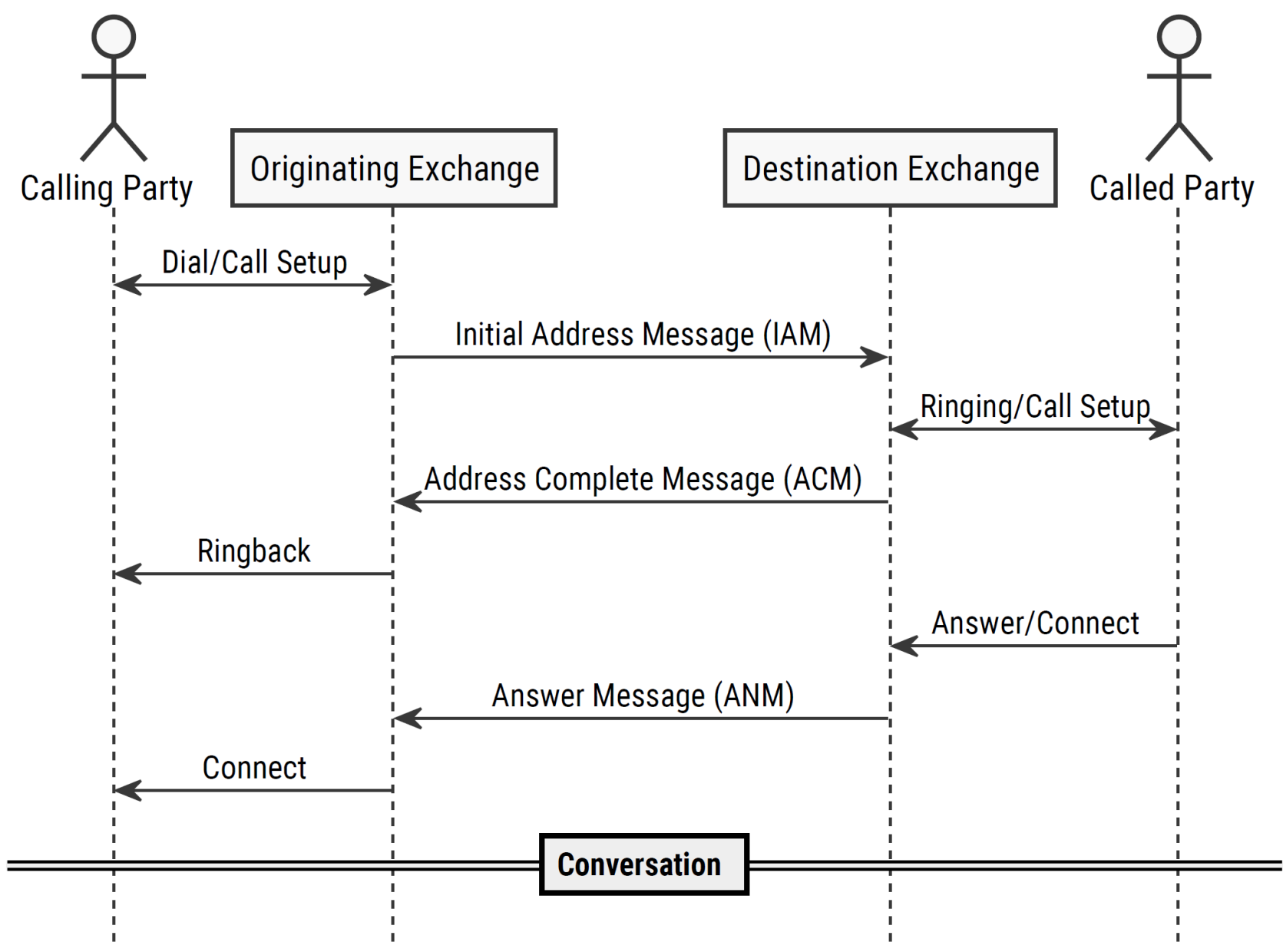


✔ PayPal

3:02 PM

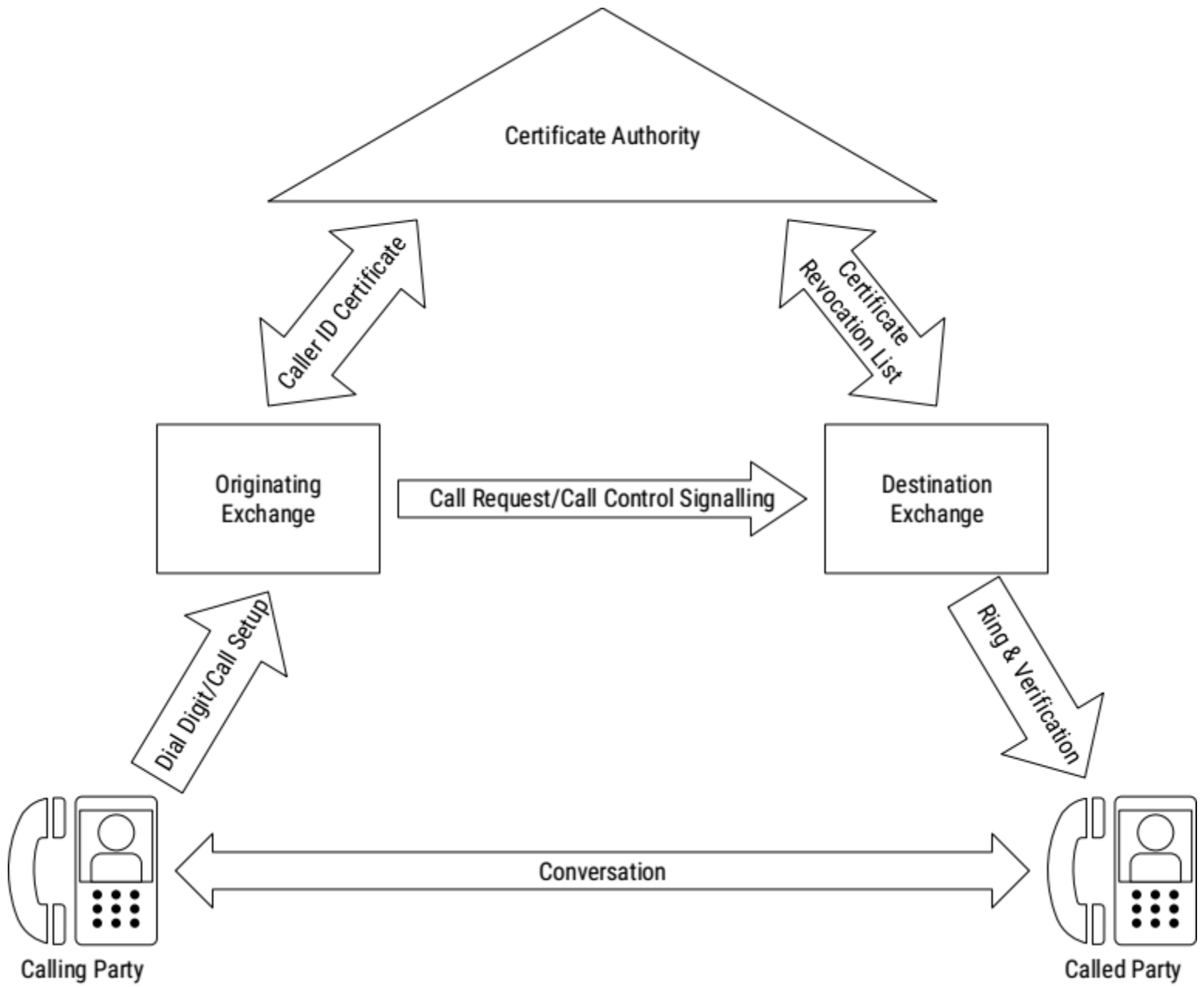
Your account information has been upda...

Designing the Verification Scheme



Design Principles

- Authentication
- Integrity
- Deployability

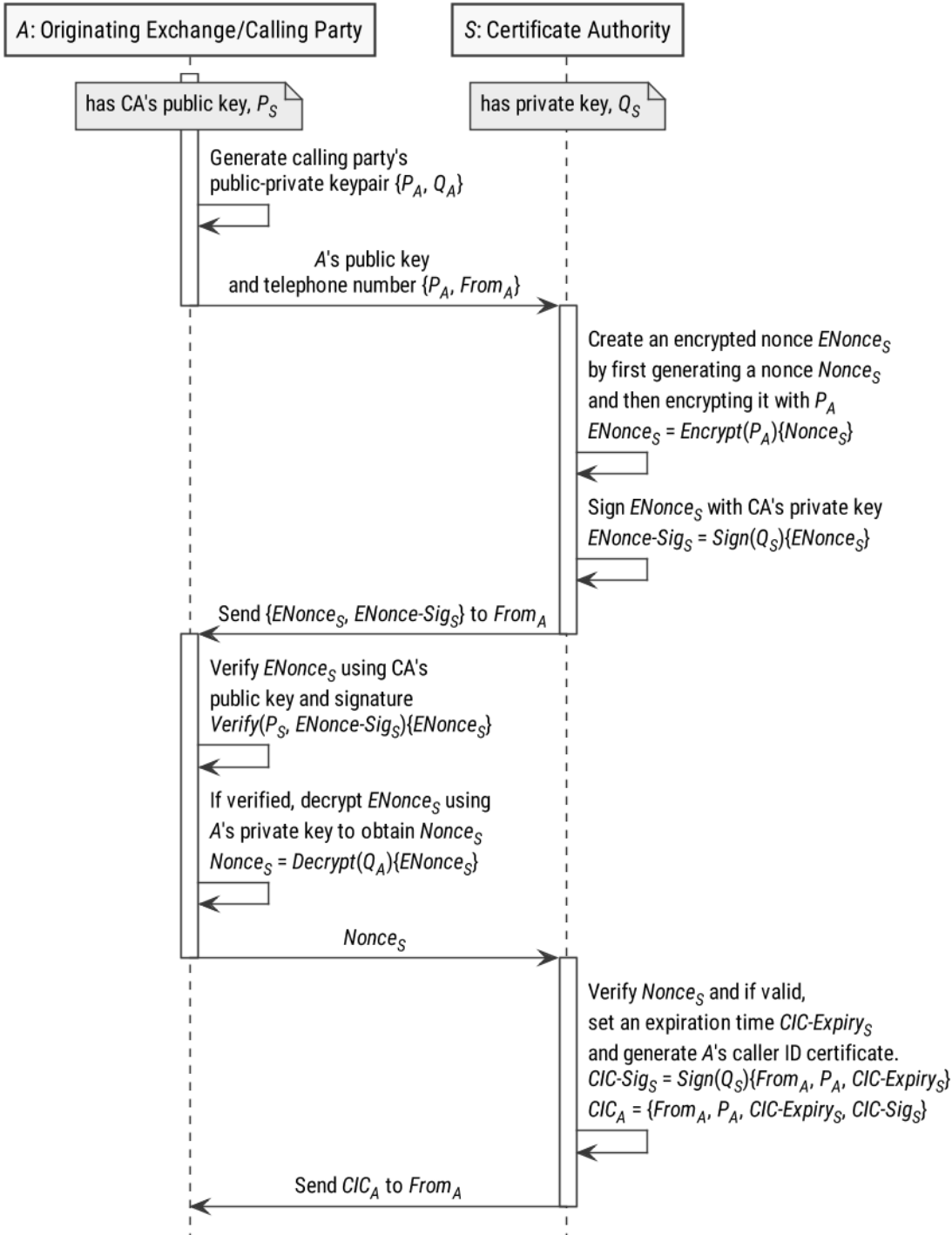


Scheme Overview

1. Caller ID Verification
2. Authenticated Call Request

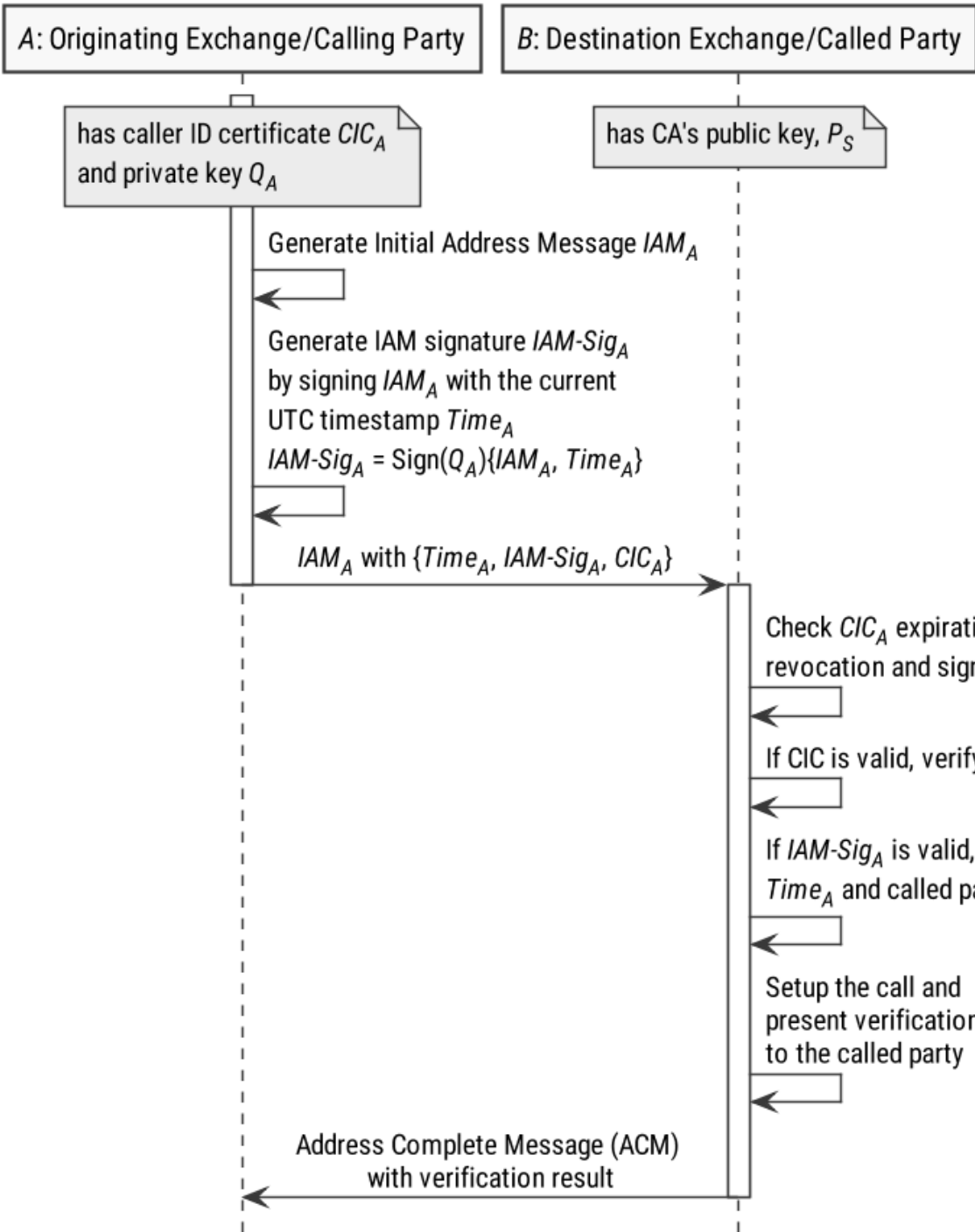
Caller ID Verification

- Provide proof of E.164 ownership to a CA
- Obtain a short-term Caller ID Certificate
- Use caller ID to generate Authenticated Call Requests



Authenticated Call Request

- Assert the originating identity
- Generate an extended IAM with a digital signature using the Caller ID Certificate
- Validate both the IAM signature as well as the signer



Other Details

- UTC Timestamp (UNIX time)
- X.509 certificate format
- International E.164 format
- Parameter Compatibility Information parameter (Q.764.2.9.5.3.2)

Parameter	Type	Length (octets)
UTC Timestamp	Optional Part	4-?
Signature Algorithm	Optional Part	1-?
Signature	Optional Part	16-?
Caller Identity Certificate	Optional Part	32-?

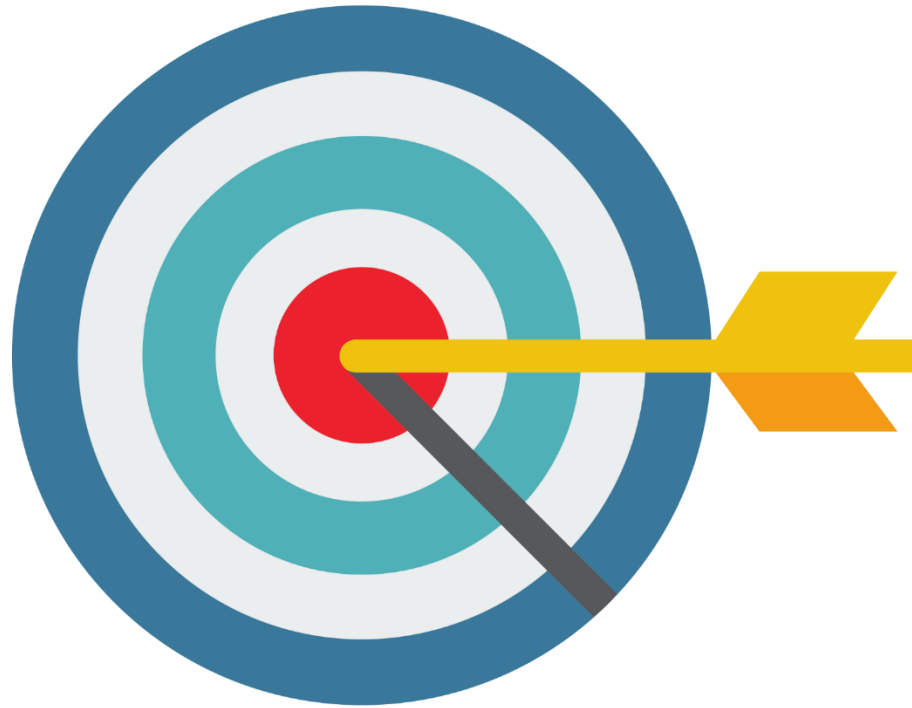
Security Considerations

- Certificate Revocation to guard against stolen identity
 - E.g. stolen certificate, cell phone theft, etc.
- Recommend using Certificate Revocation List (CRL) with short-term certificates
 - No stalling, OCSP can cause stalling
 - Risk containment
 - Reduce list size

Local Deployment Considerations

- Presenting the security indicator to the called party
- Use a flag indicator, only if
 - local exchange network connection is secured
 - identity of the local exchange carrier is authenticated
 - the call request header is integrity protected
- Otherwise recommend using full conversion of the extended IAM parameters to allow the called party's user equipment to perform verification







Acknowledgement





ITU Kaleidoscope 2016
ICTs for a Sustainable World

Thank You

Huahong Tu
Arizona State University
tu@asu.edu

Download paper:
<http://huahongtu.me/publications/itu-callerid.pdf>

Bangkok, Thailand
14-16 November 2016