Why the Equifax Breach Should Not Have Mattered

Marten Lohstroh
University of California, Berkeley

World Congress on Internet Security
December 12, 2017, Cambridge, UK

This work was supported in part by TerraSwarm, one of six centers of STARnet, a Semiconductor Research Corporation program sponsored by MARCO and DARPA.

Berkeley UNIVERSITY OF CALIFORNIA | EE CS

About the Author

Marten Lohstroh is graduate student at the University of California, Berkeley, advised by Prof. Edward A. Lee

Research Interests: cyber-physical systems, models of computation, programming languages, and systems design.

Currently mostly working on *composability in IoT systems*.

(see: http://accessors.org)

Public Outcry

Equifax hack: 44 million Britons' personal details feared stolen in major US data breach (The Telegraph)

THE EQUIFAX BREACH EXPOSES AMERICA'S IDENTITY CRISIS (Wired)

Equifax Says Cyberattack May Have Affected 143 Million in the U.S. (NY Times)

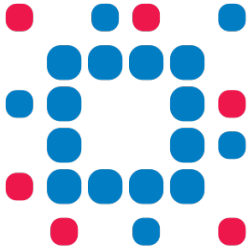
Equifax faces legal onslaught from US states over data breach (Financial Times)

The Many Problems With Equifax's Response To The Privacy Breach Crisis (Forbes)

Canada's privacy commissioner opens probe into Equifax data breach (CBCNews)

Protect our Personal Data!

Where *is* the Data?



Experian

acxiom

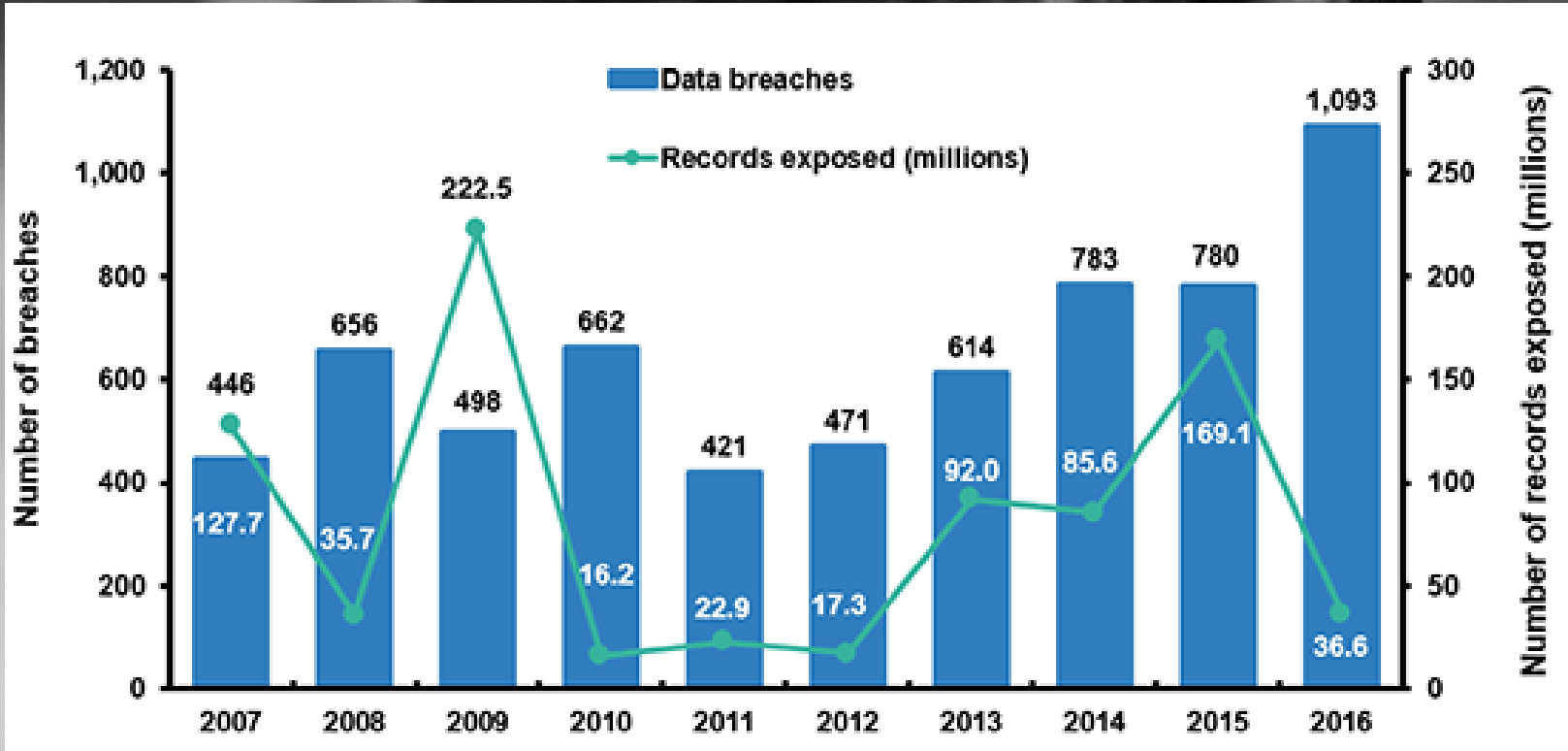
EQUIFAX

AllianceData

TransUnion

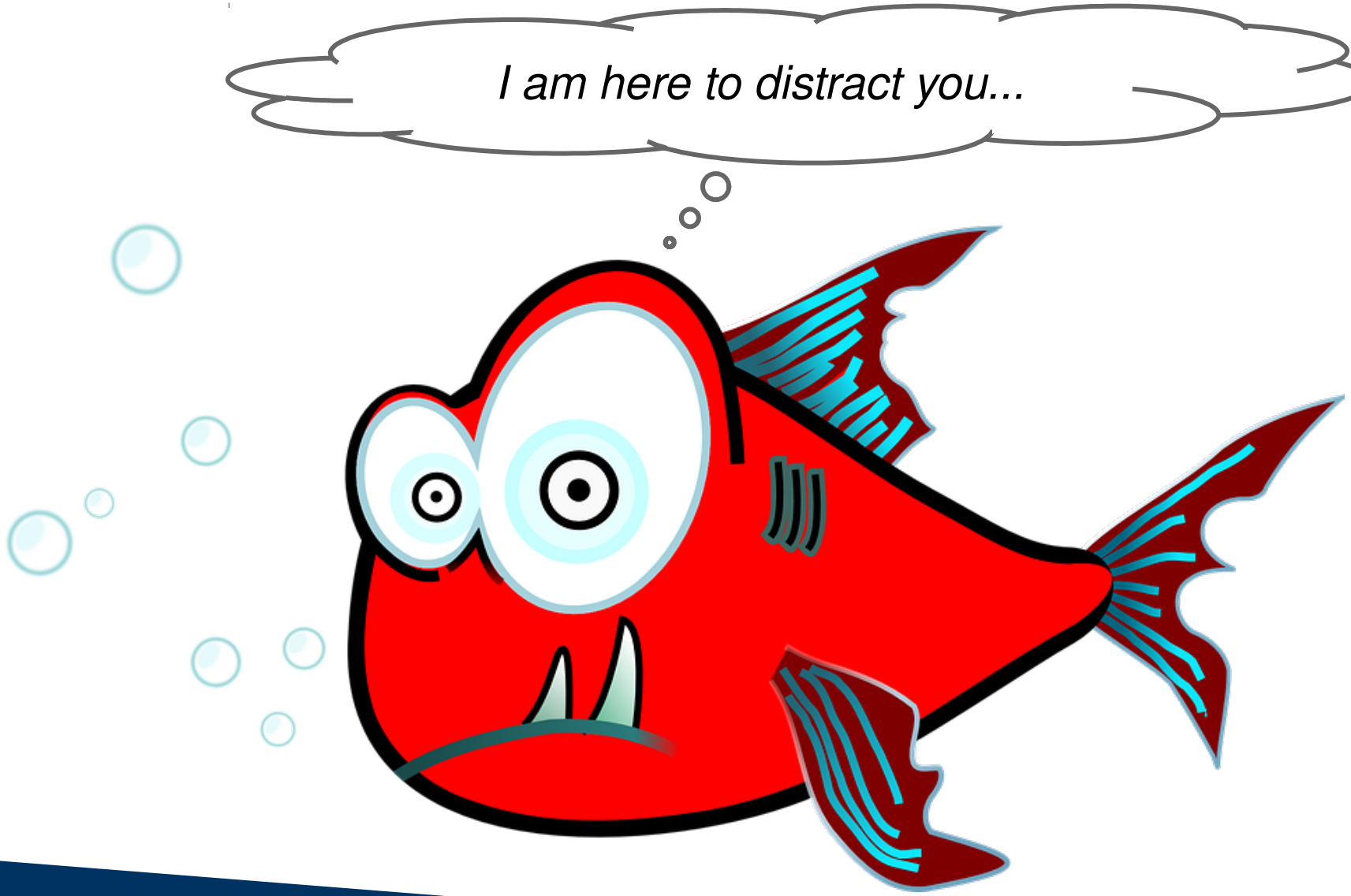
Berkeley UNIVERSITY OF CALIFORNIA | EE CS

Murphy's Law



Source: Identity Theft Resource Center.

Berkeley UNIVERSITY OF CALIFORNIA | EE CS


I am here to distract you...

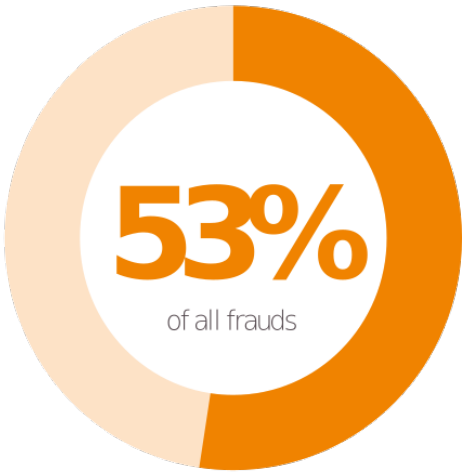
Identity Fraud (UK)

Almost

173,000

highest level ever recorded

Represents over



78%

committed using victim's current address

96%

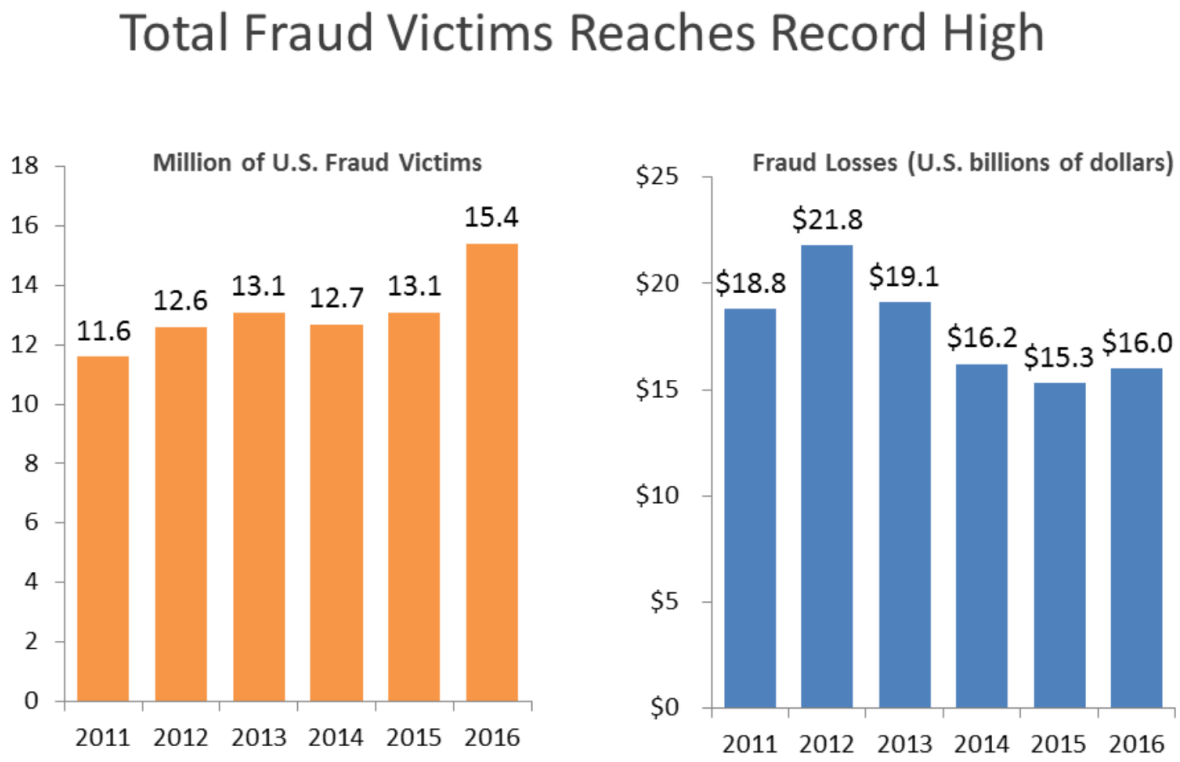
committed with genuine victim's identity

9/10

fraudulent applications for bank accounts and f nancial products made online

Source: Fraudscape 2017, Cifas

Identity Fraud (USA)

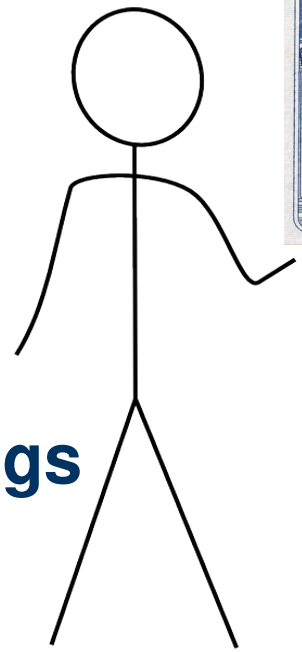


Source: 2017 Identity Fraud Study, Javelin Strategy & Research.

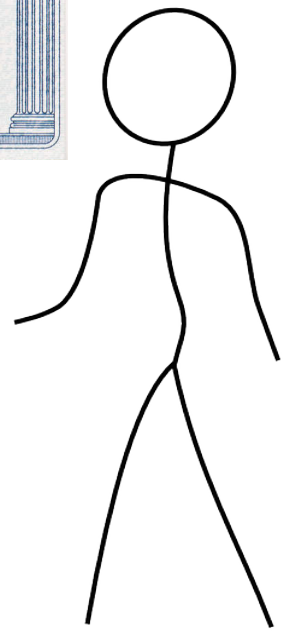
Poor Authentication of Identity Claims

✓ Verify that the information **is correct**

☒ Verify that the information **belongs to the subject**

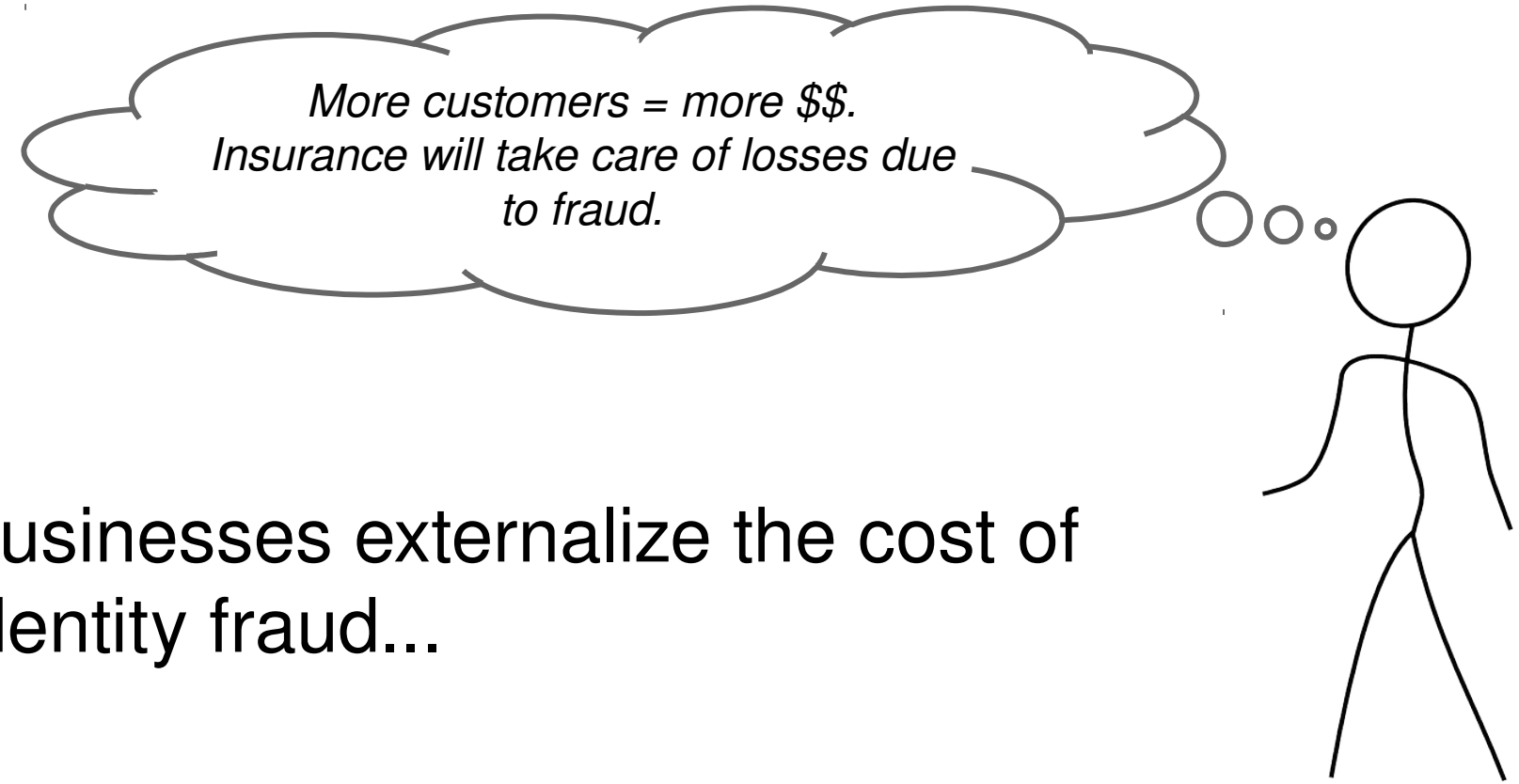


Mallory (Subject)



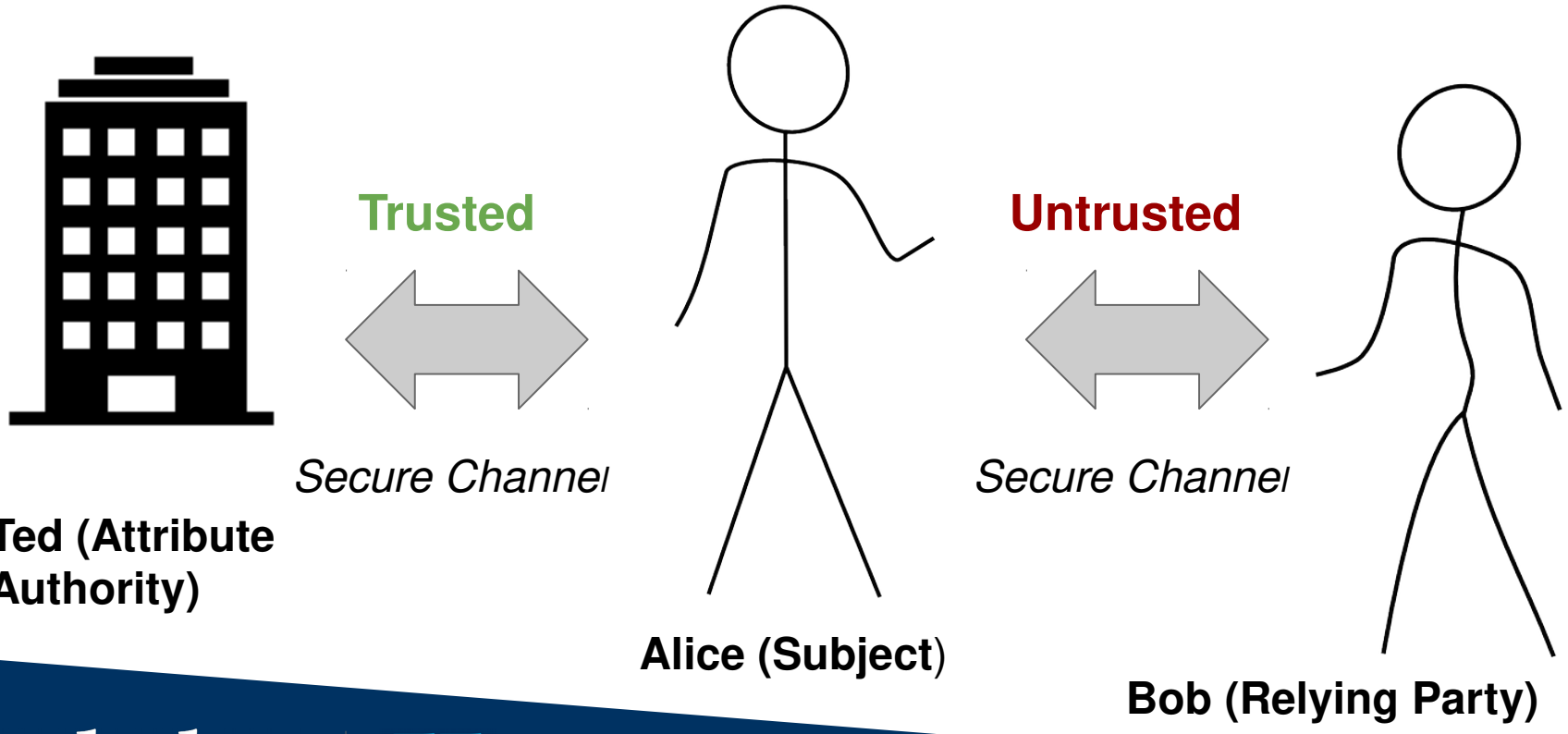
Bob (Relying Party)

Why such Poor Standards?

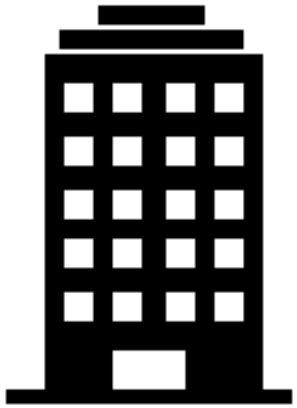


Businesses externalize the cost of identity fraud...

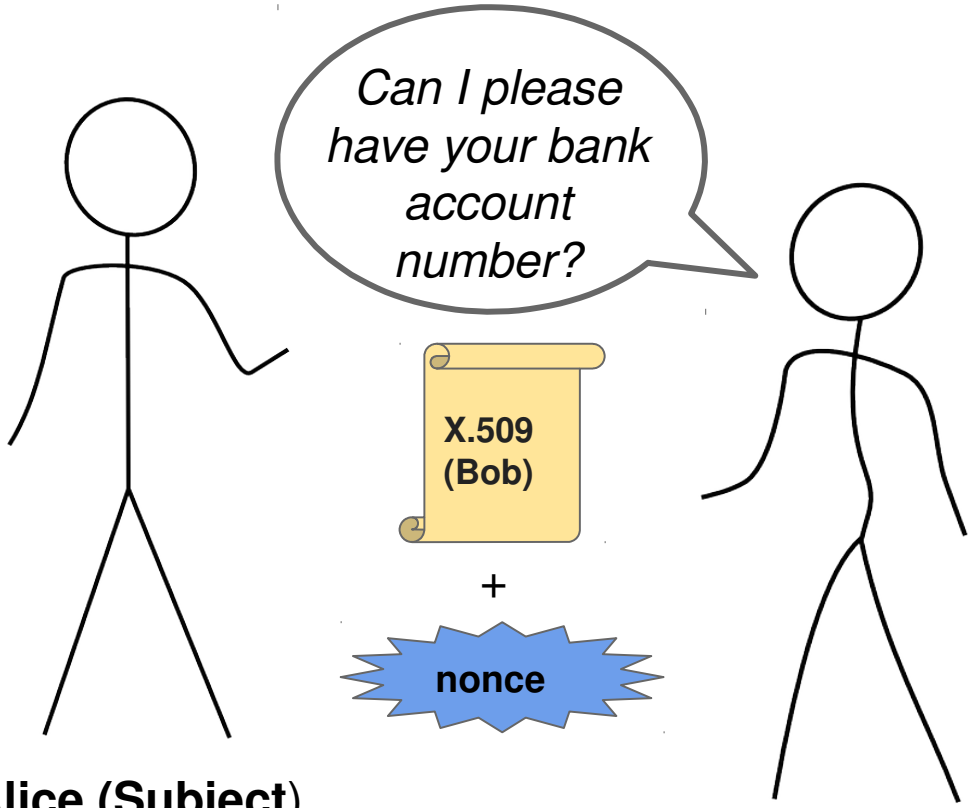
Certified Identity Claims



CIC Protocol Sequence



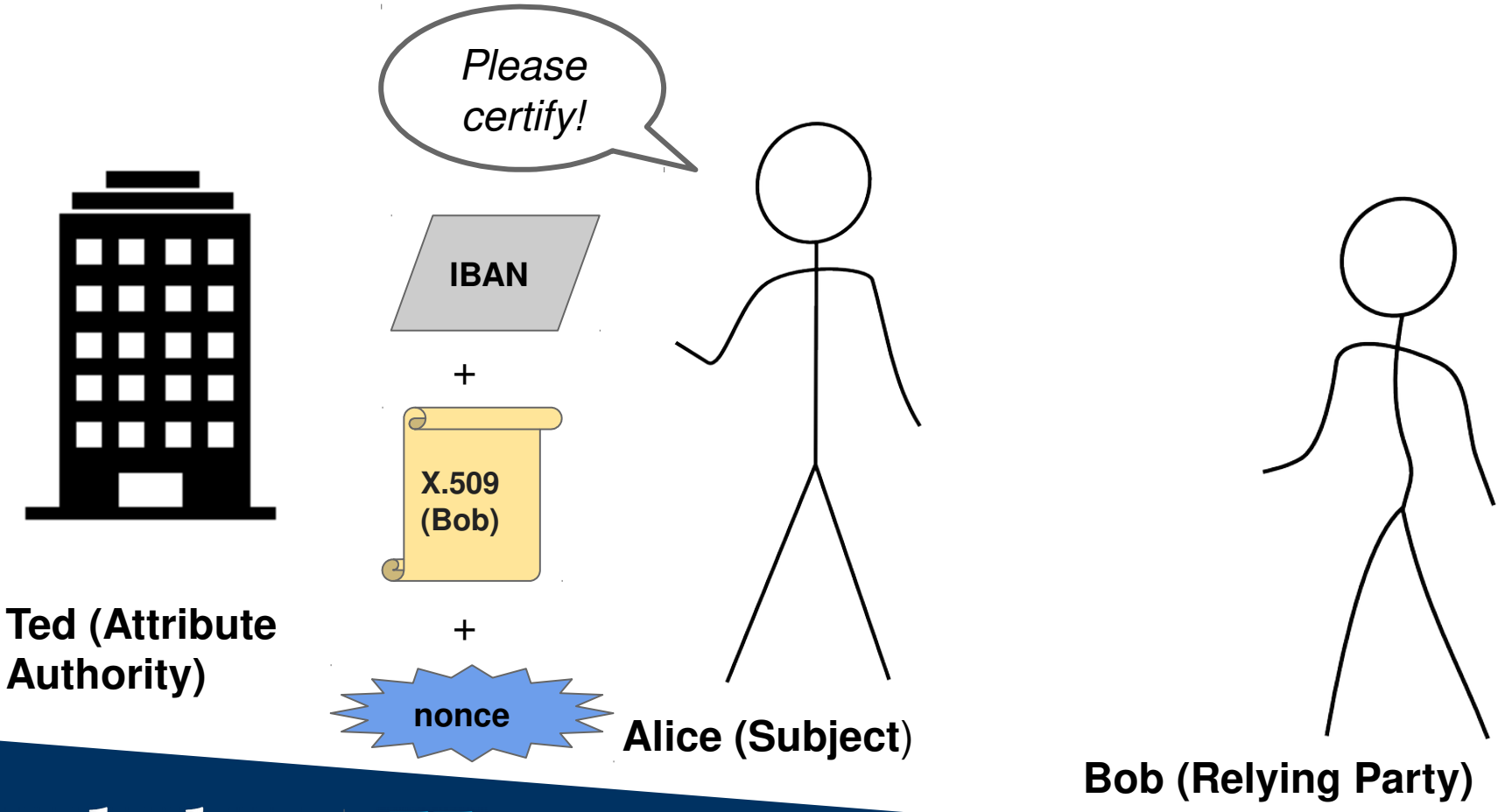
Ted (Attribute Authority)



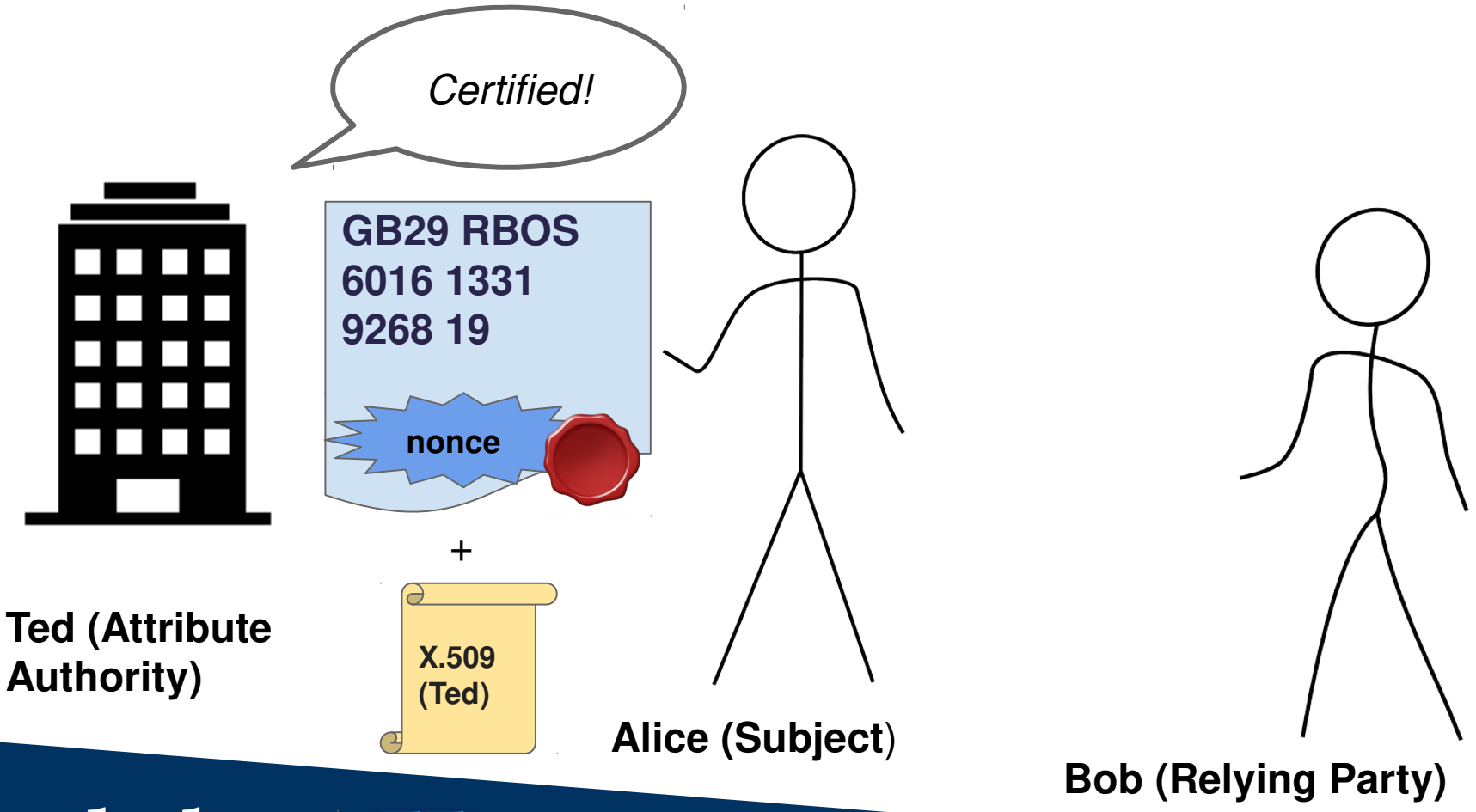
Alice (Subject)

Bob (Relying Party)

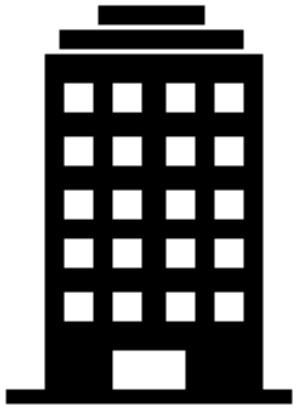
CIC Protocol Sequence



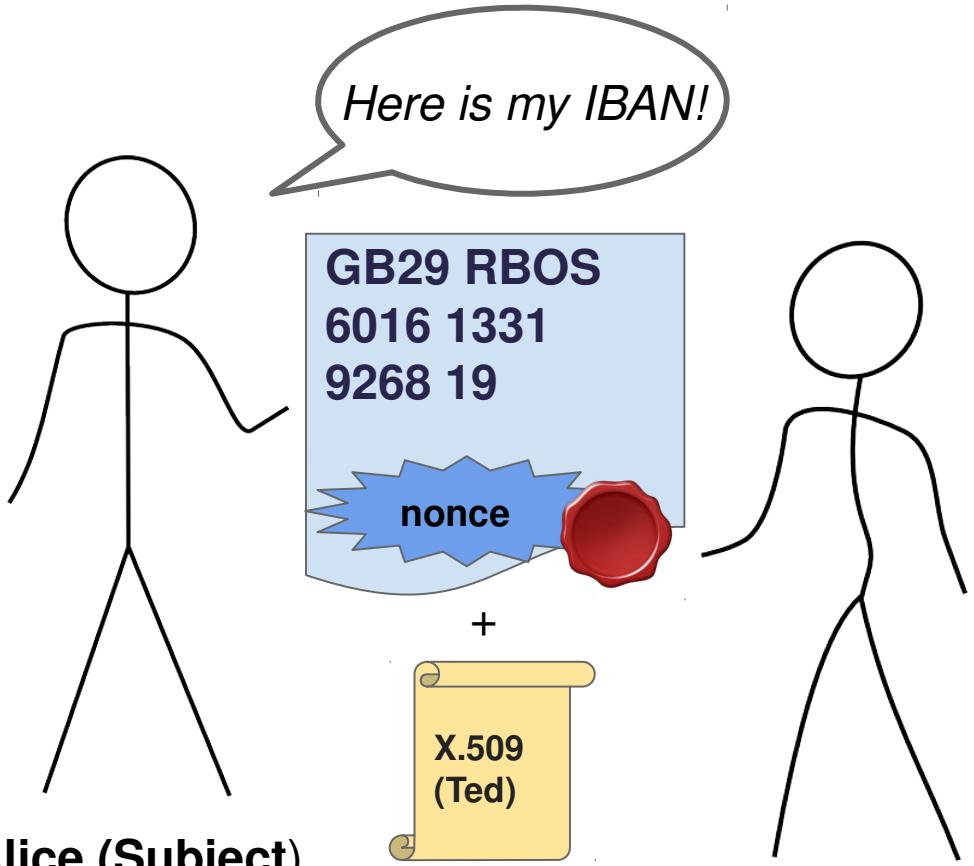
CIC Protocol Sequence



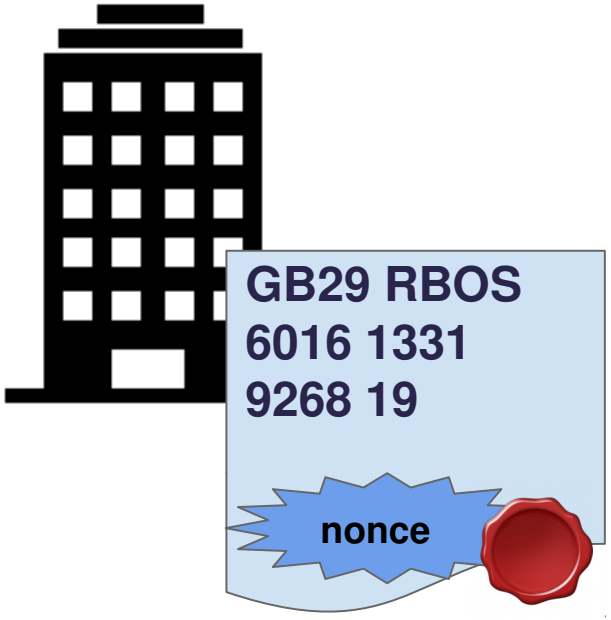
CIC Protocol Sequence



Ted (Attribute Authority)

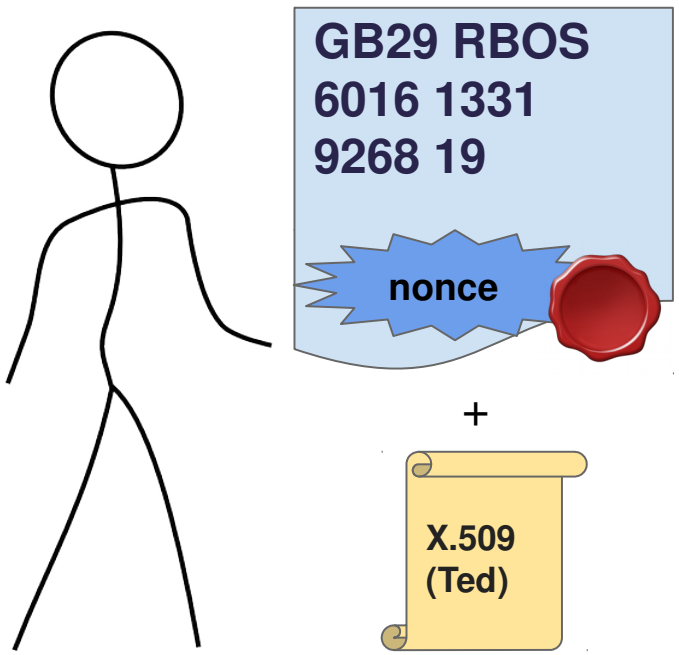


Cryptographic Details



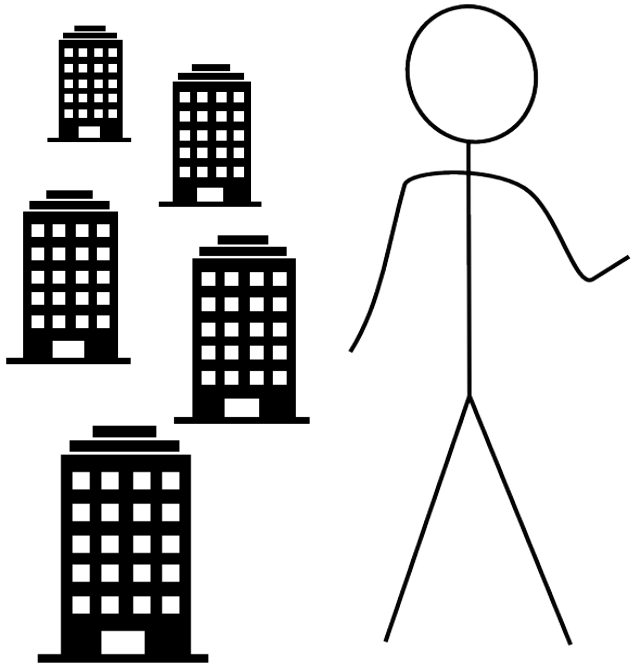
Step 1: Encrypt claim with public key of Relying Party.
Step 2: Sign the result with private key of Attribute Authority

Security



- CIC is meaningful only if Bob trusts Ted;
- Certification occurred at Bob's request (check nonce);
- Bob cannot use the obtained CIC to impersonate Alice.

Privacy



Alice (Subject)

- Alice may simply deny Bob's request;
- There is no direct communication between Bob and Ted;
- Ted, however, will learn about Alice's interaction with Bob.

Characteristics and Limitations

- Simple, decentralized, and scalable;
- Can be implemented using off-the-shelf technology and Web standards (e.g., RSA, HTTPS, X.509);
- Trust between Subject and Attribute Authority is essential.

Implementation and Adoption

- Standardization of a data format/ontology for requests and responses;
- Willingness of corporations to adopt the technology:
  - May require new laws/enforcement

Questions?