

# Establishing and Protecting Digital Identity in Federation System

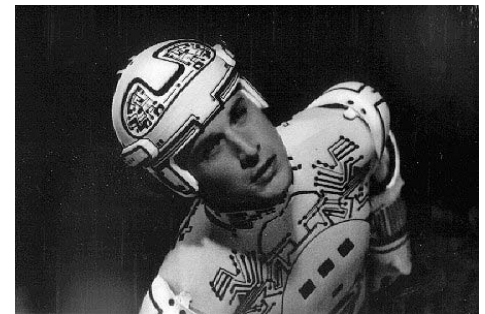
Abhilasha Bhargav-Spantzel  
Anna C. Squicciarini  
Elisa Bertino

# Outline

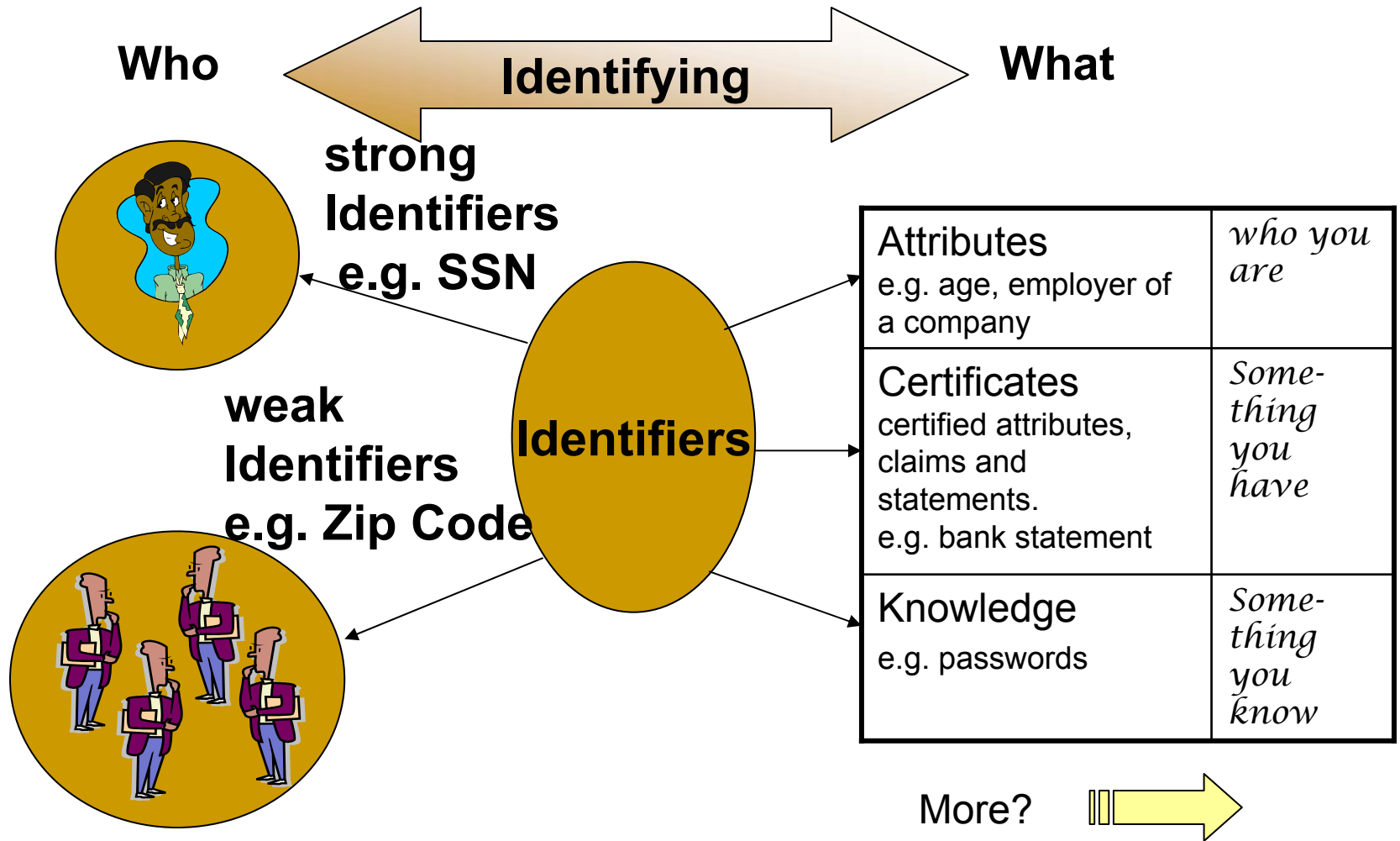
- Preliminary Concepts
  - Establishing Unique Identifiers
  - Identity Theft
    - Main Issues
    - Our Solution
  - Conclusion
-

# Preliminary Concepts

- **Digital Identity:** A set of claims made by a person or a thing about itself or another digital subject
- **Claim:** An assertion of the truth of something, typically one which is disputed or in doubt. It may be represented by an **identifier**:
  - ❑ Knowledge of a secret
  - ❑ Personally identifying information
  - ❑ Membership in a given group (e.g. people under 16)
  - ❑ Capability



# Identification



*Identification is the process of mapping claimed attributes of an individual to his/her associated identifier.*

# Federation

- An association of organizations that use a common set of attributes, practices and policies to exchange information about their users and resources in order to enable collaborations and transactions

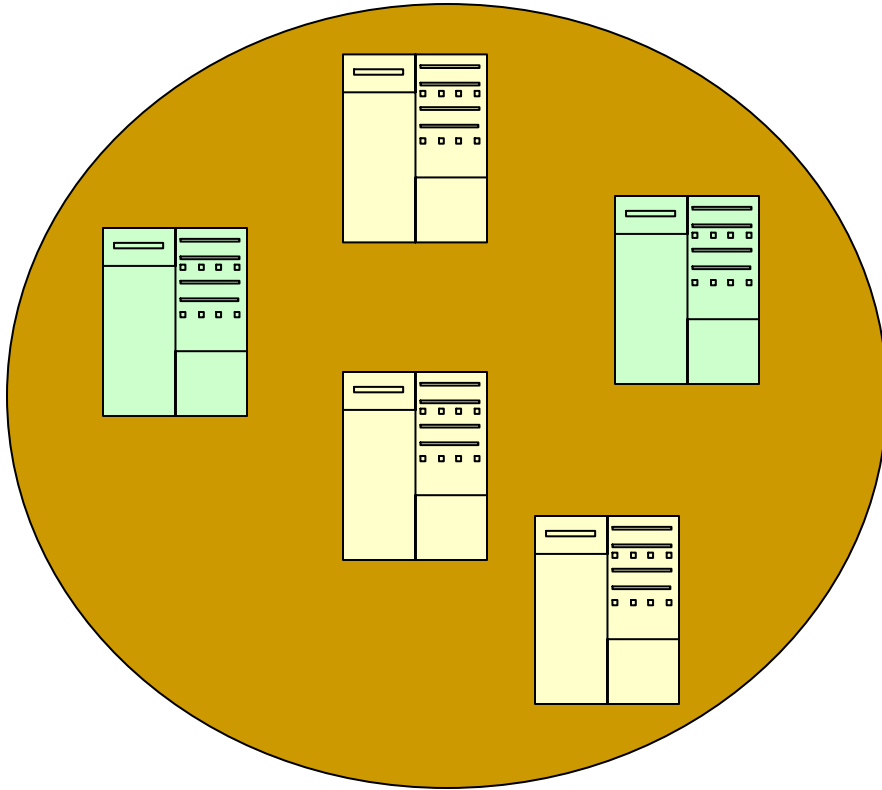
# Preliminary Concepts [cont.]

- Main Entities in a Federation
  - Service Providers
  - Identity Providers
  - “Users”
  
- Two principles:
  - “Least revealing means”
  - “Most convenient means”

# Outline

- Preliminary Concepts
- Establishing Unique Identifiers
- Identity Theft
  - Main Issues
  - Our Solution
- Conclusion

# How do we start?



# Establishing Unique Identifiers

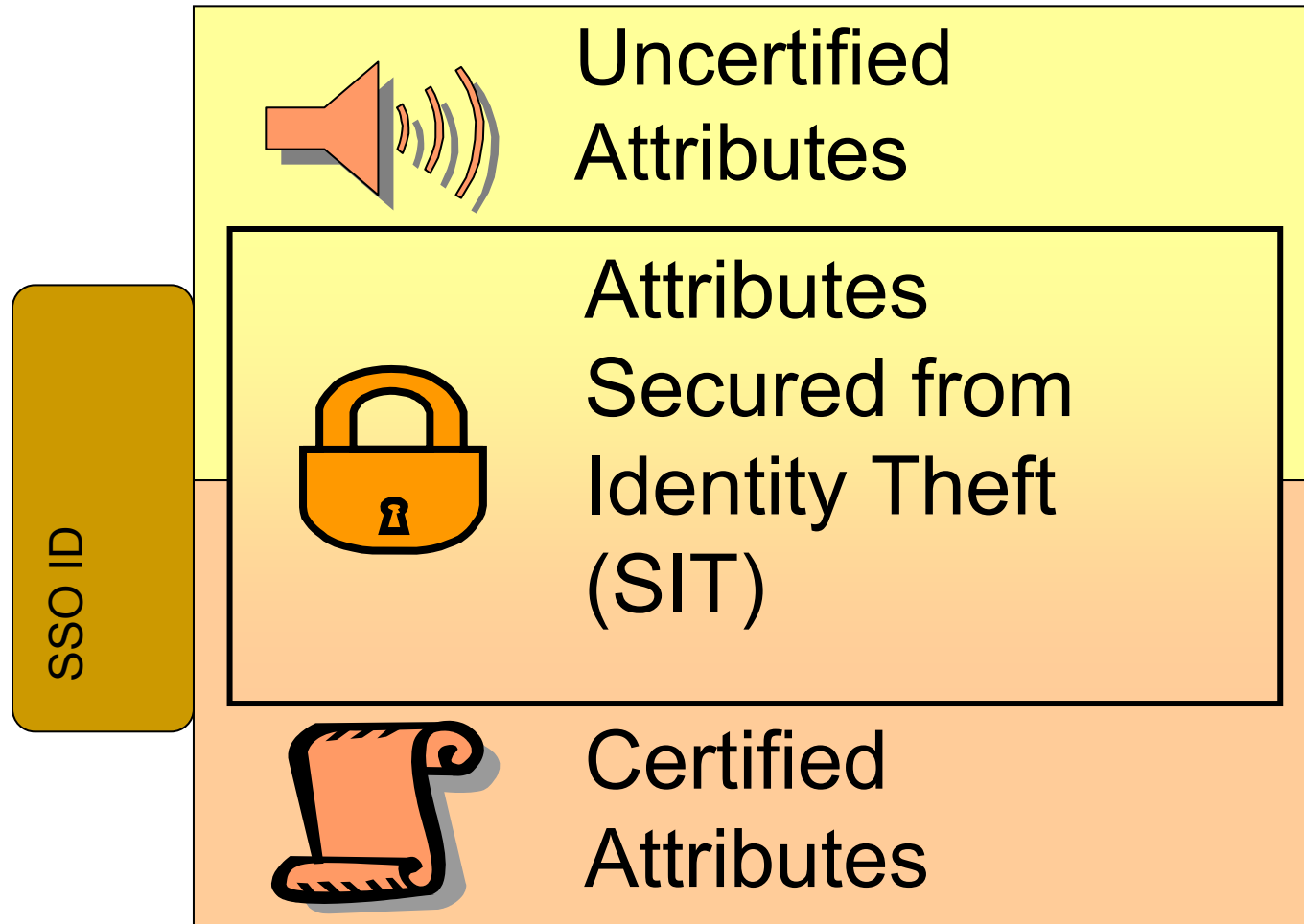
## ■ Service Providers

- ❑ Every SP has public and private key pair
- ❑ Group public key

## ■ Users

- ❑ Establishing Single Sign-On (SSO)  
e.g. : Alice@SP1 vs. Bob\$SP1
- ❑ Followed by **attributes** (Identifiers)

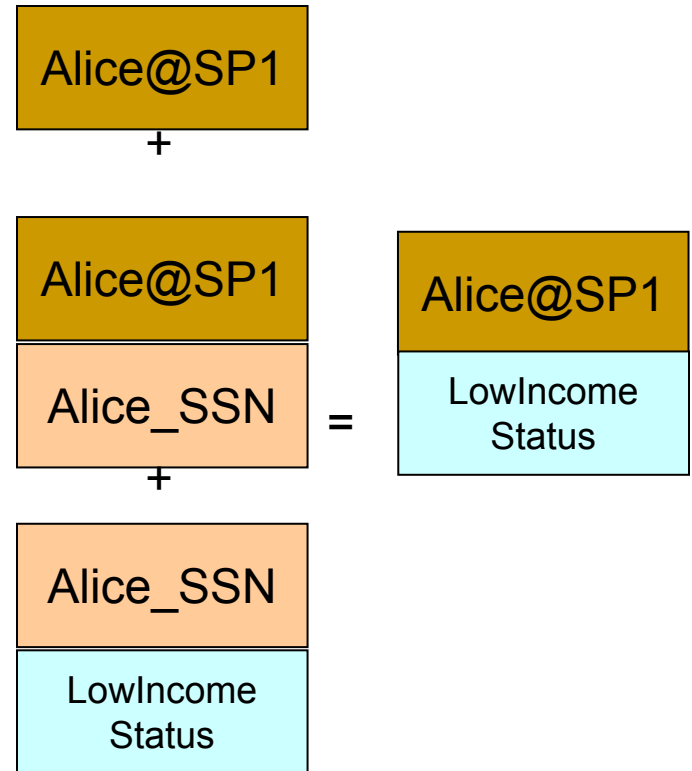
# Attribute types



# Part 1: Attributes

## (Uncertified and Certified)


- Uncertified: Voluntary and user claims
- Certified
  - Certificates Issued by external authorities
  - Federation IdP:
    - A. Credential Ownership
    - B. Issuance of new Credentials



# Part 2: Attributes Secured from Identity Theft [Main Idea multi-factor]

Require additional identity information (like mother maiden name or SSN) as **proof** to qualify to be the owner of the identity attribute being used (like credit card number)

**Example Real Life Scenario:** Requirement for additional proofs of identity



I will use my credit card to pay

To use your credit card please show your **drivers license** and an additional photo id for verification of your identity



# Challenges in the digital world

- **Verification** of user identity online is hard.
  - Register and store, a priori, the digital identifiers of a user with a **registrar**
- However an honest user does not want to
  - Store sensitive value in clear
  - Give additional identity information



# Outline

- Preliminary Concepts
  - Establishing Unique Identifiers
  - **Identity Theft**
    - Main Issues
    - Our Solution
  - **Conclusion**
-

# Problem of Identity Theft

- **Identity Theft** is the use of personally identifying information belonging to one individual by another individual for financial or personal gain
- Main Problem:  
*Lose Control of Your Own Identity*
  - Easy for identity thieves to **assert they are someone else** with the right data
  - Difficult for Identity Theft victims to **prove that they are themselves** once compromised
  - There is already a lot of information of an individual available at different places

# Obtaining Identity Information

- Online Phonebooks
  - <https://find.intelius.com/>
- Google
- Forms filled

# One Solution

- Establish and use a **proof of identity** associated with the actual identifier
- Use more than one such proofs of separate identifiers thus providing **multi-factor authentication**
- Preserve user privacy
- Use the information in the federation for detecting identity theft attacks

# 2 Main Phases

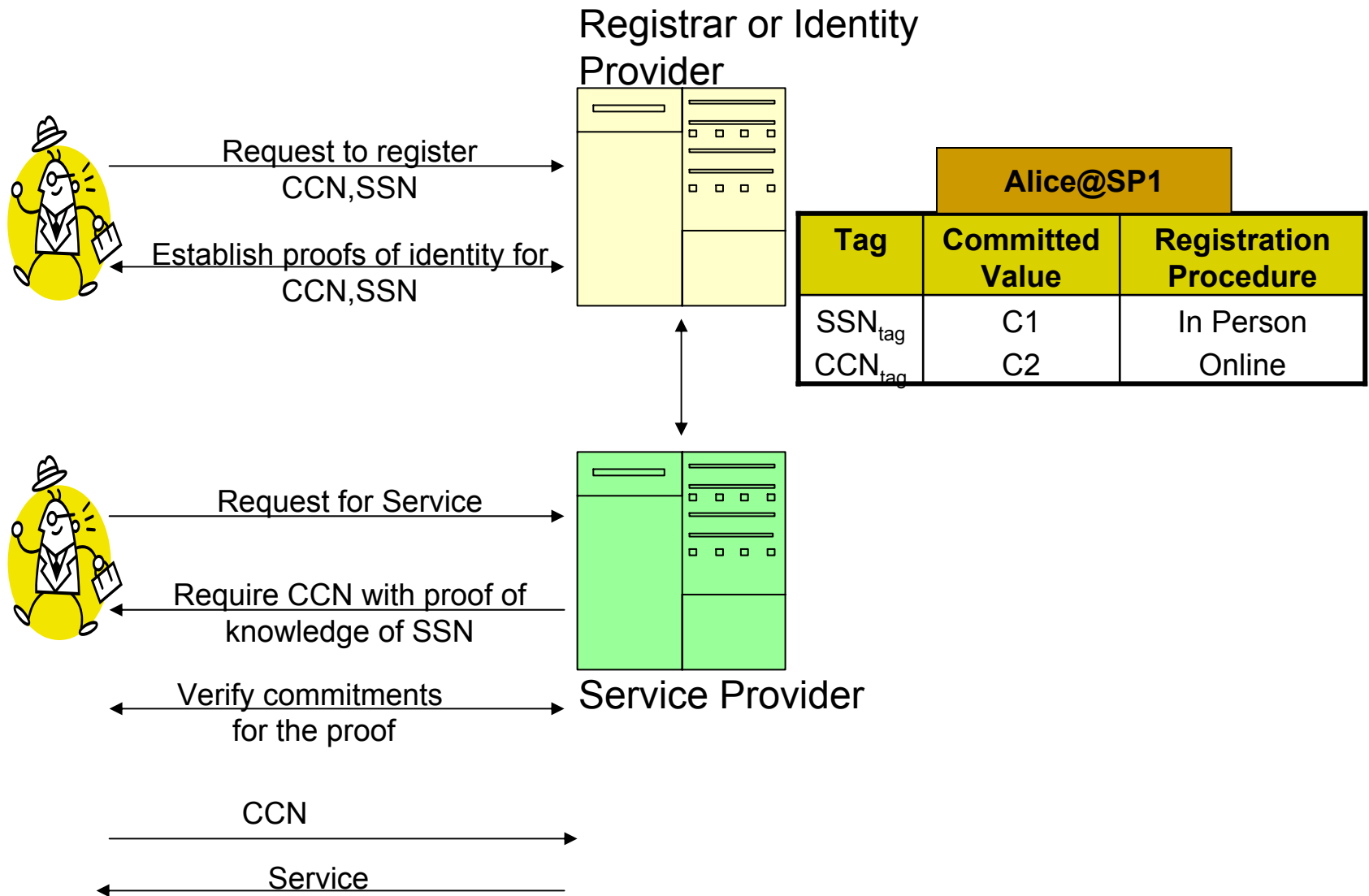
## ■ Bootstrapping or Registration

- Here the user **commits** his strong identifiers to be used later as proofs of identity. These are the SIT attributes.

## ■ Usage

- Before revealing the actual value of a SIT attribute one has to verify the commitments of other SIT attributes as *proofs of identity*.

# Example



# Registration Phase

- Two types of registration

- In-Person Registration
- Online Registration

- What is registered?

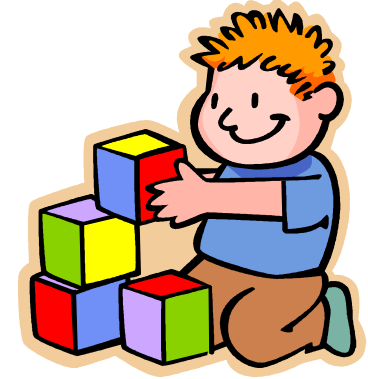
- **Commitments** corresponding to the strong identifier
- This will be used later as a proof in the opening phase of the zero knowledge protocol

- Have to check for **duplicates!**

Alice@SP1		
Tag	Committed Value	Registration Procedure
SSN <sub>tag</sub>	C1	In Person
CCN <sub>tag</sub>	C2	Online

# Building blocks

- Zero Knowledge Proof
- Distributed Hash Tables



# Briefly -- Zero Knowledge Proofs

- **Prover** tries to prove a certain fact to the other party, called the **verifier**.
- An **interactive proof** usually takes the form of a challenge-response protocol
- **Zero knowledge.** The verifier learns nothing about the fact being proved (except that it is correct) from the prover that he could not already learn without the prover
  - Verifier cannot even later prove the fact to anyone else.

# Schnorr Protocol (ZK Proof of Discrete Log)

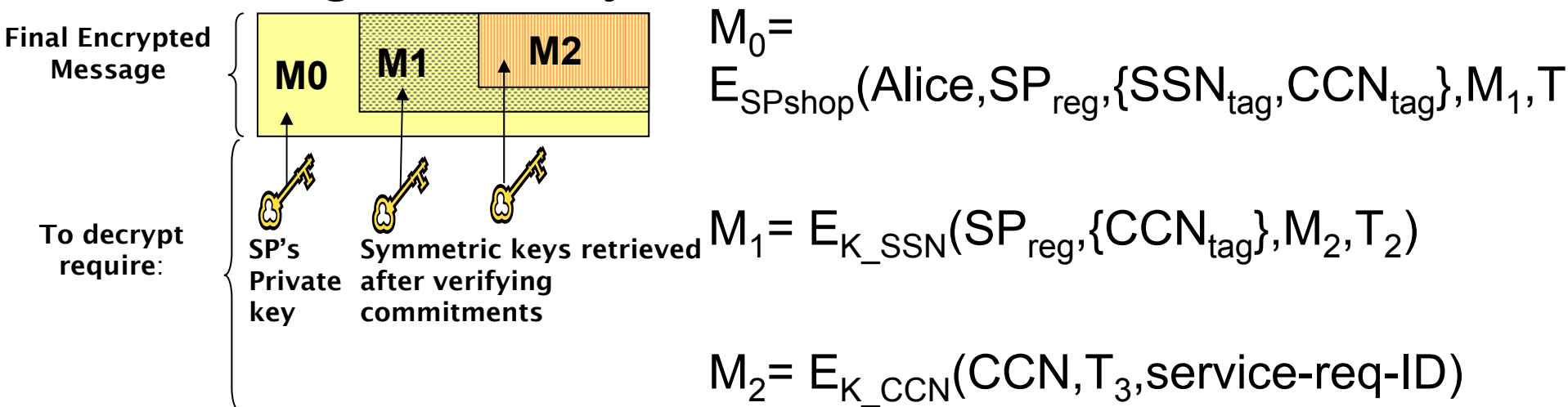
- System parameter:  $p, q, g$ .  $q \mid (p-1)$  and  $g$  is an order  $q$  element in  $\mathbb{Z}_p^*$
- Public identity:  $c$
- Private authenticator:  $a$  where  $c = g^{-a} \pmod p$
- Protocol
  1. P: picks random  $r$  in  $[1..q]$ , sends  $d = g^r \pmod p$ ,
  2. V: sends random challenge  $e$  in  $[1..2^t]$
  3. P: sends  $y = r + ea \pmod q$
  4. V: accepts if  $d = g^y c^e \pmod p$

# How to detect duplicates in a Federation?

- Put the strong identifiers in a hash table and look for collisions
- Problem: How can thousands of hosts cooperatively maintain a large hash table in a completely decentralized fashion?
- Answer: Distributed Hash Tables

# Usage Phase

- Modified the proof of the ZKP such that with each successful proof of commitment a symmetric key was generated
- These keys were used to encrypt the final message in a layered fashion



# What are the main advantages?

- The actual values of the registered attributes used as proofs do not have to be stored
- One step towards assurance of valid information in a federation. Distributed hash tables used, prevent a malicious user to register stolen attributes.
- At the time of usage proof of knowledge of additional identifiers was mandated. This provides
  - Privacy
  - Multi-factor authentication

# Outline

- Preliminary Concepts
- Establishing Unique Identifiers
- Identity Theft
  - Main Issues
  - Our Solution
- **Conclusion**

# Conclusion:

- Contributions:
- Step by step procedure on how a user can establish and then use his/her digital identity in a federation.
- **Identity theft** protection mechanism which uses *secure message exchange protocols* and tools like *cryptographic zero knowledge proofs* and *distributed hash tables*.
- Formal detailed analysis of the security and complexity our solution

# Current and Future Work

- Formal description of the model with detailed desiderata
- Improved and efficient ZKP and other cryptographic techniques needed to satisfy the defined properties
- Implementation and testing of proposed solution on open source Shibboleth Identity system

# Thank You!

bhargav@cerias.purdue.edu

# Problem: Paradoxical Requirements

- Property 1: *Identity Hiding*. Given  $f(x)$ , it is infeasible to compute the value of  $x$ .
- Property 2: *Duplicate Detection*. Given  $f(x)$  and  $f(y)$  identify the case when  $x = y$ .

