# 14. Scenario I: Your Credentials Please

*Paul Syverson*

## Introduction

Under this scenario the tools of anonymity serve the ends of business and e-government. Service providers can only link transactions to identifiers of individuals when needed for a specific service. These identifiers generally are not linkable to each other: They are service-specific. Most transactions are authorized without the need for even these identifiers by means of anonymous credentials. For example, a person can show that she is authorized for a service as a county resident, or as a veteran, or as disabled, or as having some combination of these without needing to identify herself.

Remote access to services is made over anonymity preserving infrastructures, such as onion routing (Dingledine et al. 2004). Face-to-face transactions are comparable to cash transactions, except that they may be accompanied by some authenticator, for example, presenting a token, knowing a secret, having a personal physical property (biometric), or combinations of these.

## The State of Identity

There are many kinds of transactions that can be made more private and anonymous. Most obvious of these are credit transactions. Consider the largest credit transaction that most of us will make in our lives, the purchase of a home.

John buys a house.

John is 30 years old, single, and wants to buy a house. In applying for a mortgage, he presents certificates showing that the same employer has employed him for the last five years. His income has been at least $50,000.00 per year during his employment. He has been renting for the past three years

and paying (on time) $1,000.00 per month in rent. No third party can link these facts to each other. However, he can prove that these certificates are all held by the same person and can prove that he is that person. The verifier to whom he has demonstrated that proof can show that he has received such a proof, but cannot reproduce the proof by himself without John's cooperation. Thus, the verifier can show to a third party (such as an auditor) that he has adequately checked John's credentials. Nonetheless, he is not able to take those credentials he has been shown and reproduce the proof itself (so cannot try to pass as John or get credit for John's properties). (Chaum 1985, Brands 2000, Camenisch and Lysyanskaya 2001)

Unfortunately, John has a twin brother who is not as productive a citizen as John. His name is Jim. Jim is no stranger to the court system and in fact has outstanding criminal default warrants against him for not appearing in court. The last time that Jim was arrested he used John's name and social security number because he knew that he was in default and that John had no criminal record. If the local court processed Jim under John's name, he could skip out and John would be left holding the bag.

John has faithfully filed his tax returns for the past five years. This year, as in the past, he is entitled to a state and federal refund. John's state has a law that authorizes the state's department of revenue to hold state tax refunds for scofflaws, those with child support arrearages, and those with outstanding criminal default warrants.

In an earlier decade, Jim's act of unspeakable brotherly love would have succeeded: the court would have issued a default warrant in John's name. When John's bank did a routine credit check on him, the State's lien against his tax refund would pop up. When John went to the local court to clear the matter up, he would be arrested as Jim. The local court would have an imaged picture of Jim on file. Since Jim and John are twins, the imaged photograph of Jim looks like John. John would then be held without bail on the default warrants.

Fortunately John is living in a more enlightened age. As the technology to allow anonymous transactions became more pervasive, society came to realize that authentication is important. Neither the courts nor credit agencies will now respect the sloppy identifiers of an earlier age that could let someone else pass responsibility on to an innocent victim. If John had been living in the first years of the twenty first century, there is a chance that he would have both a credit problem and a criminal record that would lead to his arrest on many occasions, despite carrying documents at all times from his district attorney explaining his circumstances (Sullivan 2003).

Instead, Jim's attempt to claim that he is John is caught by his failure to properly authenticate that he is John. More significantly, the laws and incentive structures have been formed so that any future risk stemming from incorrectly associating John with this arrest would not be his but be born by those elements responsible for the misidentification, such as the credit reporting agencies. Indeed, in this future scenario the restructuring of law and