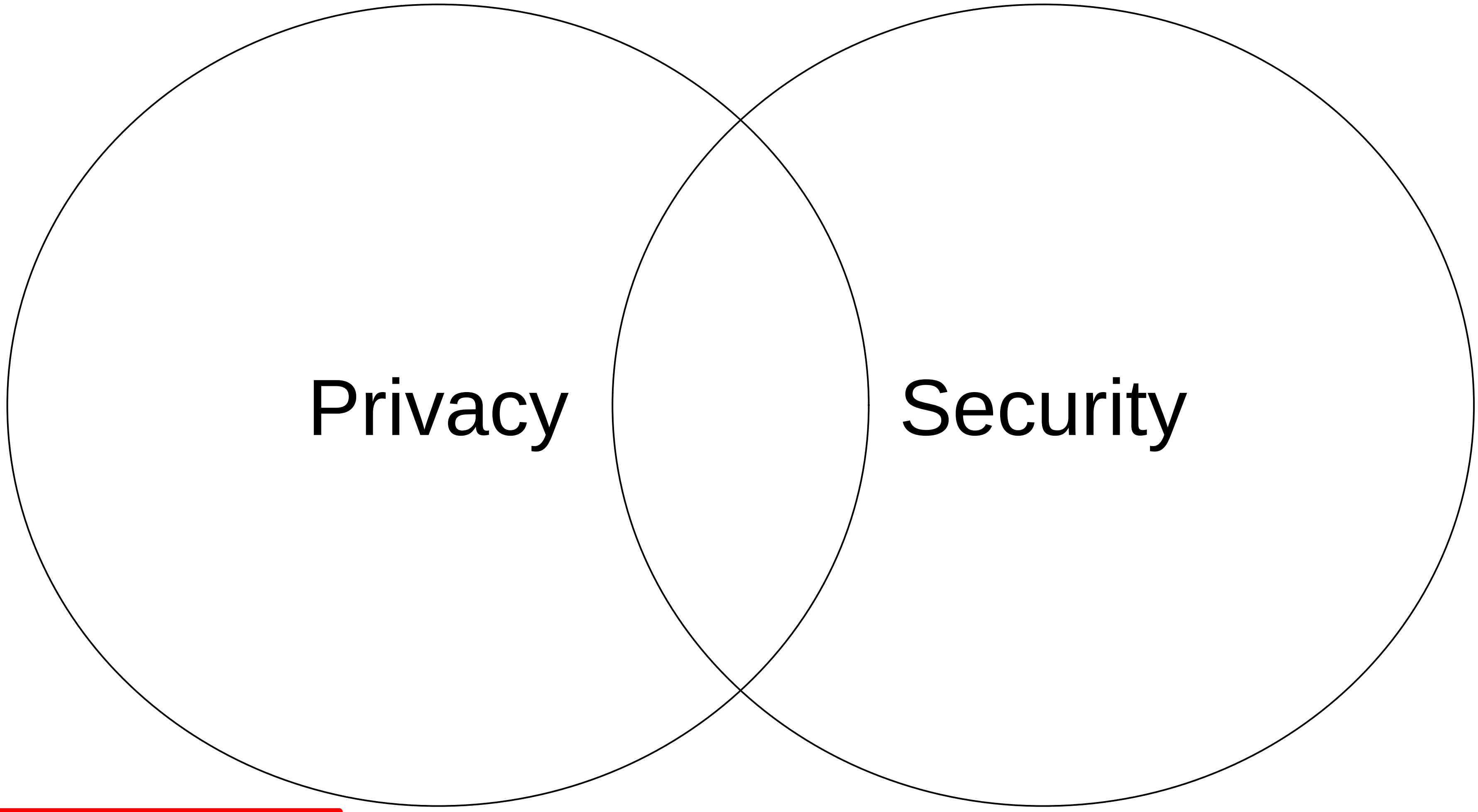
Privacy

Prof. Ravi Sandhu
Executive Director and Endowed Chair

March 8, 2013

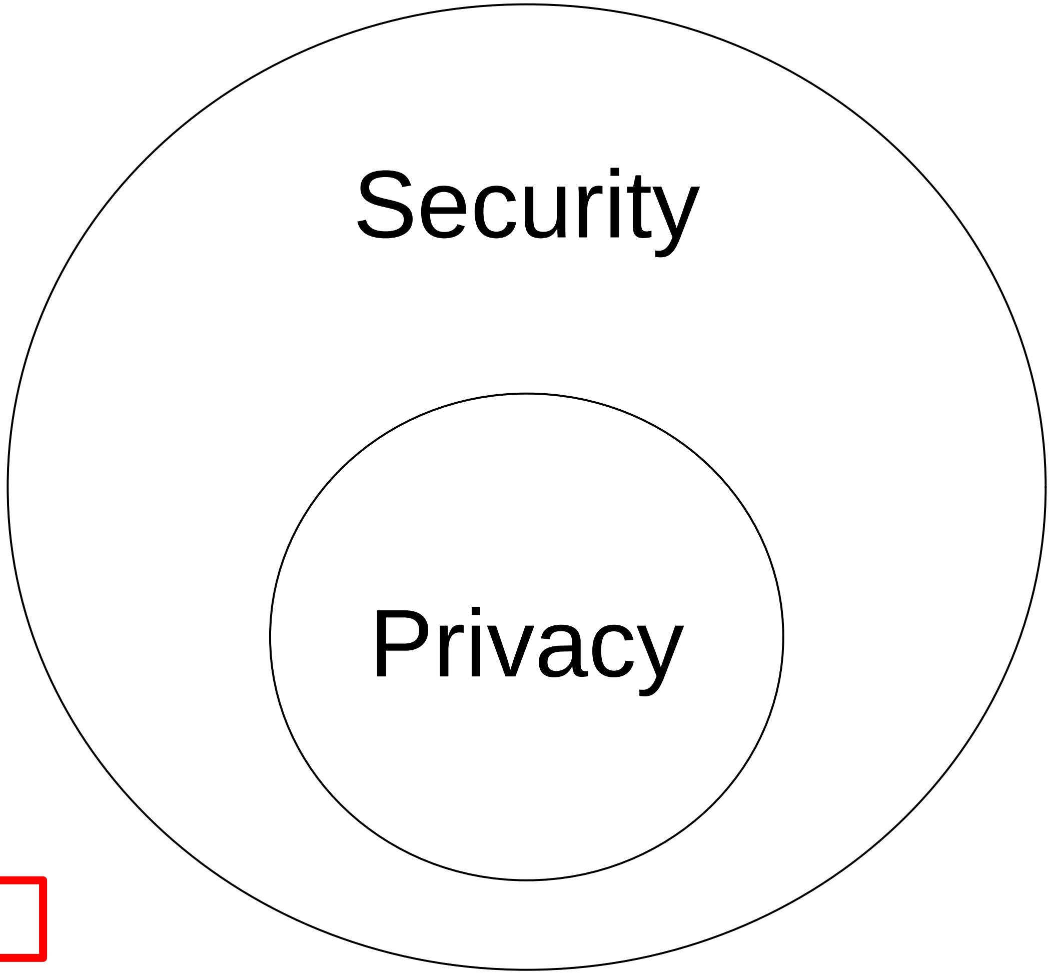
ravi.sandhu@utsa.edu
www.profsandhu.com

Privacy versus Security



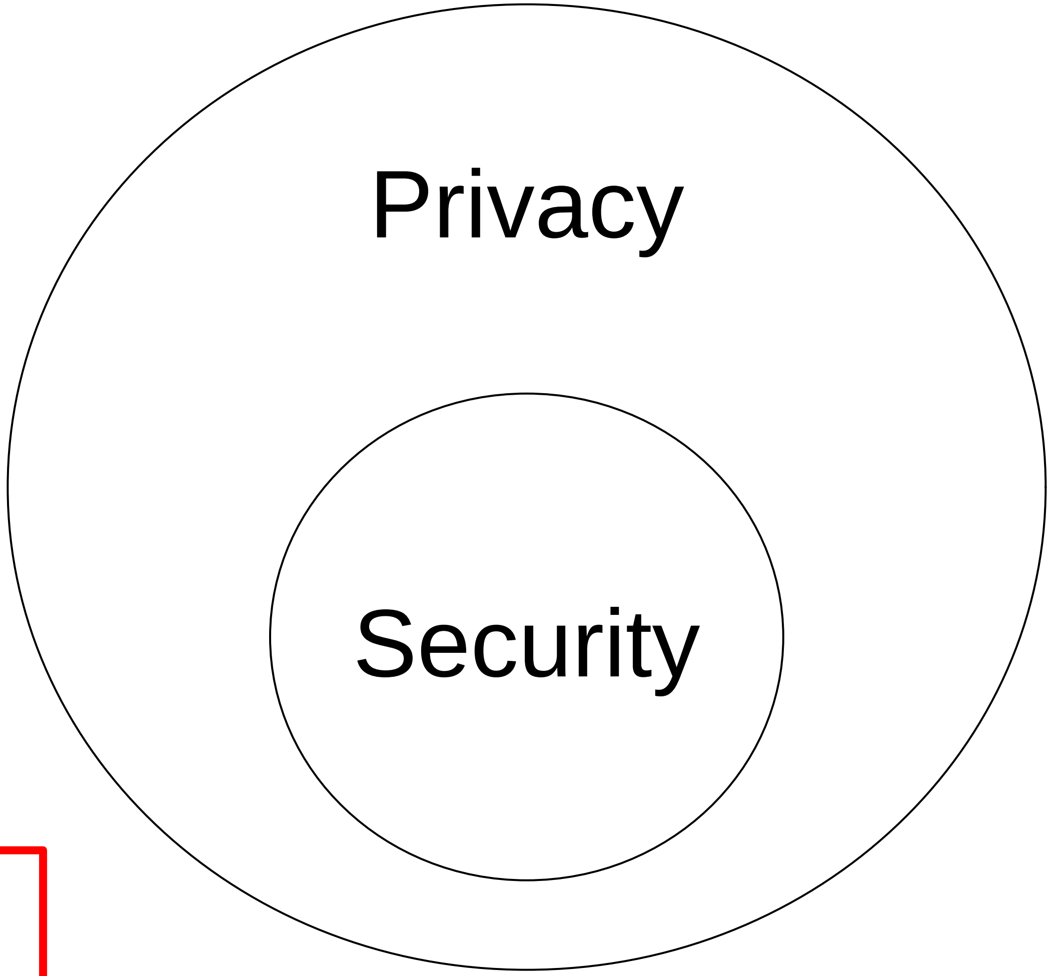
I think this is wrong

Privacy versus Security



My preferred view

Privacy versus Security

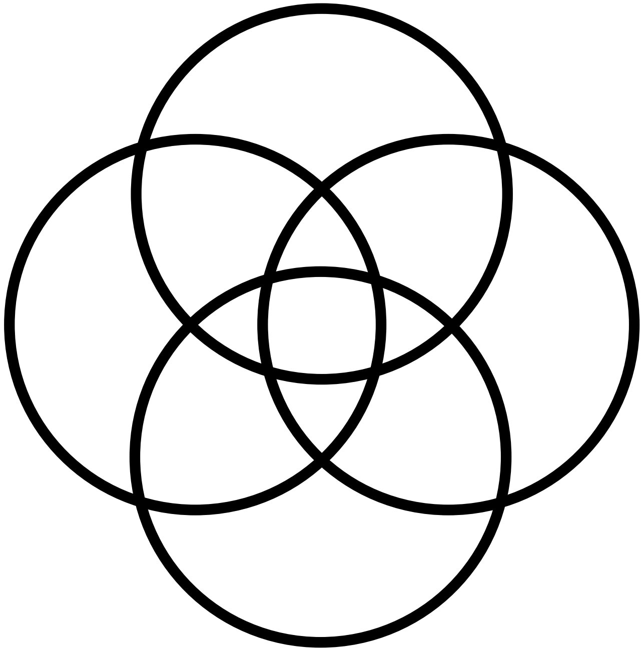


Privacy

Security

But I could be persuaded to take this view

Security Objectives



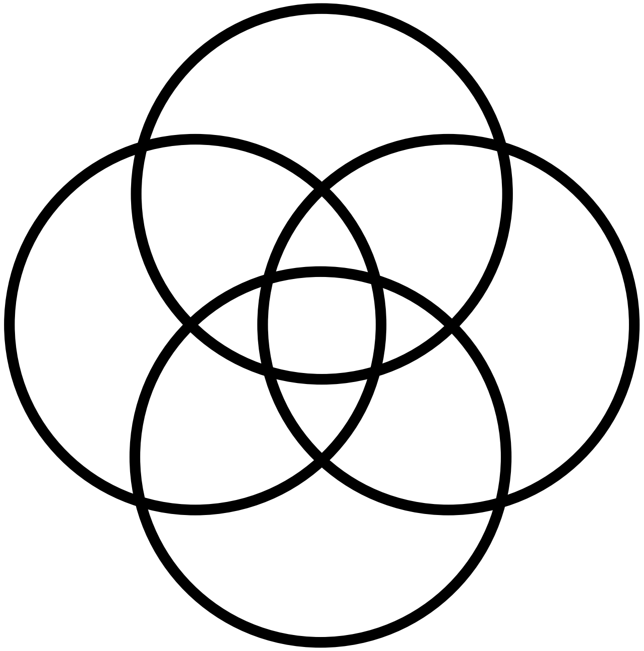
USAGE
purpose

INTEGRITY
modification

AVAILABILITY
access

CONFIDENTIALITY
disclosure

Security Objectives



USAGE
purpose

Privacy includes limits on collection and retention

Privacy includes rights to see who has accessed your privacy sensitive information

Privacy includes recourse to correct and consequently recourse to access

INTEGRITY
modification

AVAILABILITY
access

CONFIDENTIALITY
disclosure

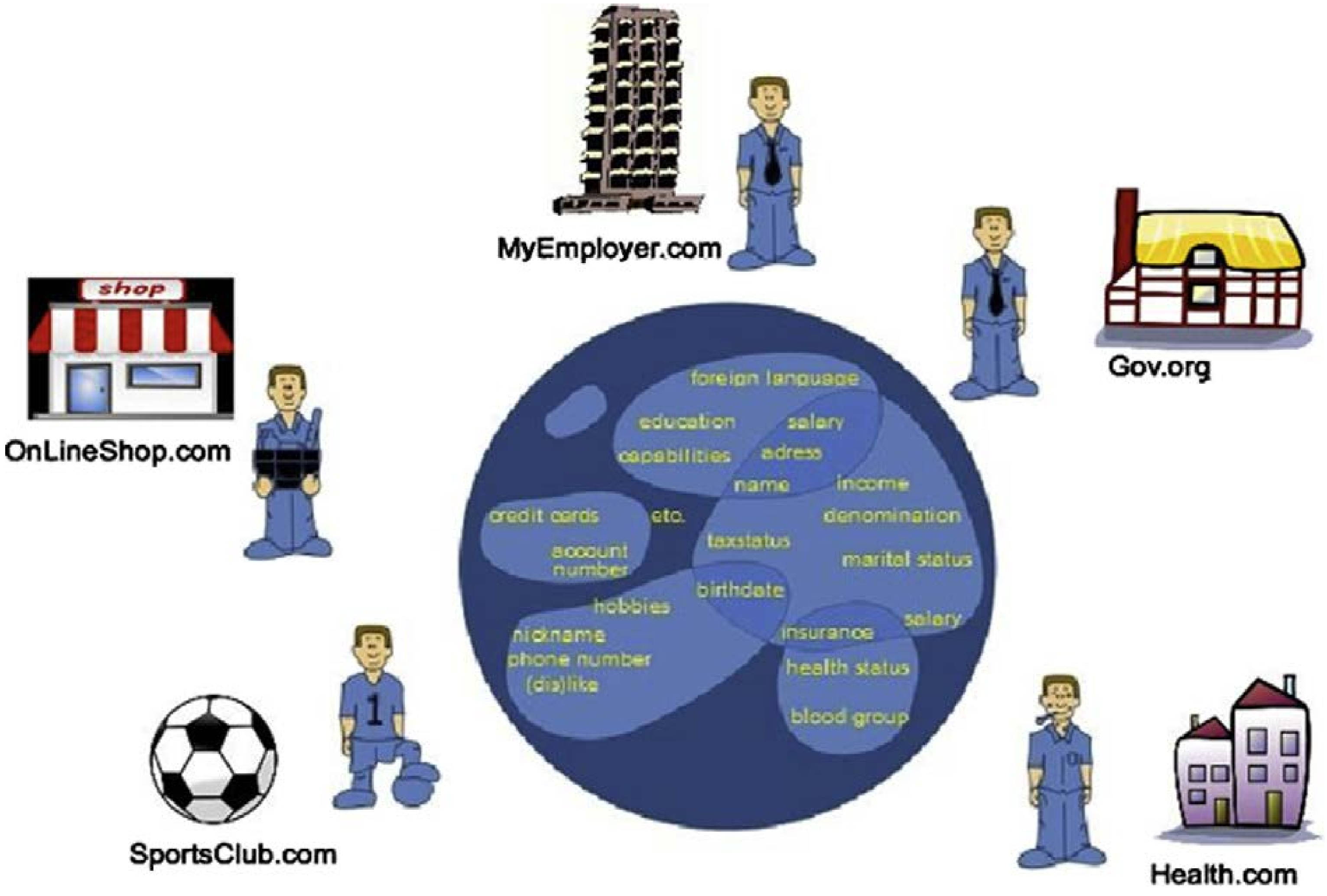
Attackers aka Adversaries

- Your nation state
- Other nation states
- Employer
- Service provider
- Friends
- Family
- Enemies
- Media
- Criminals
- …

Laws, Regulations and Standards

- Overall fragmented and slow to catch up with rapid technological change
- Privacy in the workplace is sharply limited
- Some US laws
  - FCRA (Fair Credit Reporting Act), 1970, enforced by FTC
  - FERPA (Family Educational Rights and Privacy Act), 1974
  - IRS Disclosure Laws, 1976
  - VPPA (Video Privacy Protection Act, 1988
  - HIPAA (Health Insurance Portability and Accountability Act), 1996
- A failed standard
  - P3P (Platform for Privacy Preferences) from W3C

Identity as Attributes



X.509 PKI: Identity Centric, Off-Line

VERSION

SERIAL NUMBER

SIGNATURE ALGORITHM

ISSUER

VALIDITY

SUBJECT

SUBJECT PUBLIC KEY INFO

SIGNATURE

Identity Certificate

VERSION

SERIAL NUMBER

SIGNATURE ALGORITHM

ISSUER

VALIDITY

HOLDER PUBLIC KEY INFO

ATTRIBUTES

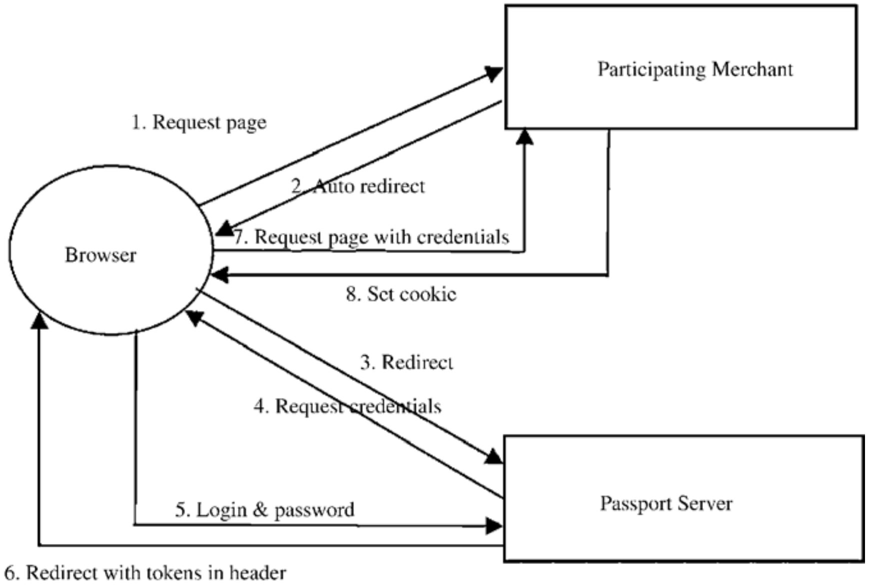
SIGNATURE

Attribute Certificate

X.509 Characteristics

- Privacy friendly
  - Certificate issuer is not involved and therefore not aware when a user receives service from a relying party UNLESS
  - Certificate revocation needs to be verified in real-time
- Privacy unfriendly
  - Identity is central
  - Attributes strongly linked through identity
  - Attributes pre-packaged into certificates

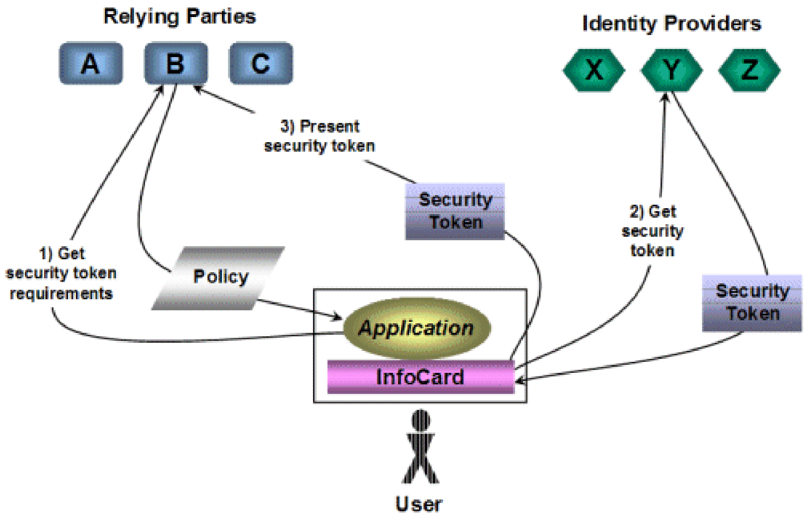
Microsoft SSO (1990's)



Knows which relying parties are being accessed

Decides which attributes to release to which relying party

Microsoft Infocard Identity Ecosystem (2000’s)



Identity Provider knows when security tokens are requested BUT does not necessarily know specific relying party

User decides which attributes to release to which relying party

Private Credentials

- Single private key
  - Multiple unlinkable public keys, generated by the user from the single private key
  - “A credential issued to one public key can be (repeatedly) transformed into a credential that’s valid on another public key of the same user. Moreover, the transformed credential can contain a selected subset of the attributes in the original credential.”
  - “Transformed credentials are unlinkable. That is, for two transformed credentials with disjoint sets of revealed attributes, you can’t tell whether they originated from the same credential or different credentials.”
  - “Instead of revealing attribute values, users can choose to merely reveal that some predicate over the attributes holds.”
  - “Private credentials also let users provide attributes in verifiably encrypted form to the relying party, so that they’re available only to a dedicated trusted third party.”

Camenisch’s Privacy Principles

1. An application should be designed so that only the minimal amount of (personal) information gets revealed to each party that is necessary for the party to perform its task.
2. Users need to be able to understand and control the usage of the information they have released.
3. All information related to users must be encrypted, both at rest and in transit.

Camenisch's Mechanism Hierarchy

1. The first type of mechanism is concerned with providing privacy at the network layer, to ensure that communication channels can be established without revealing identifying information such as IP addresses.
2. Once such communication has been established, the second type of mechanism comes into play. They allow users to reveal only information that is necessary for the task at hand.
3. The third category are mechanisms that implement special purpose applications.

3 Media Items