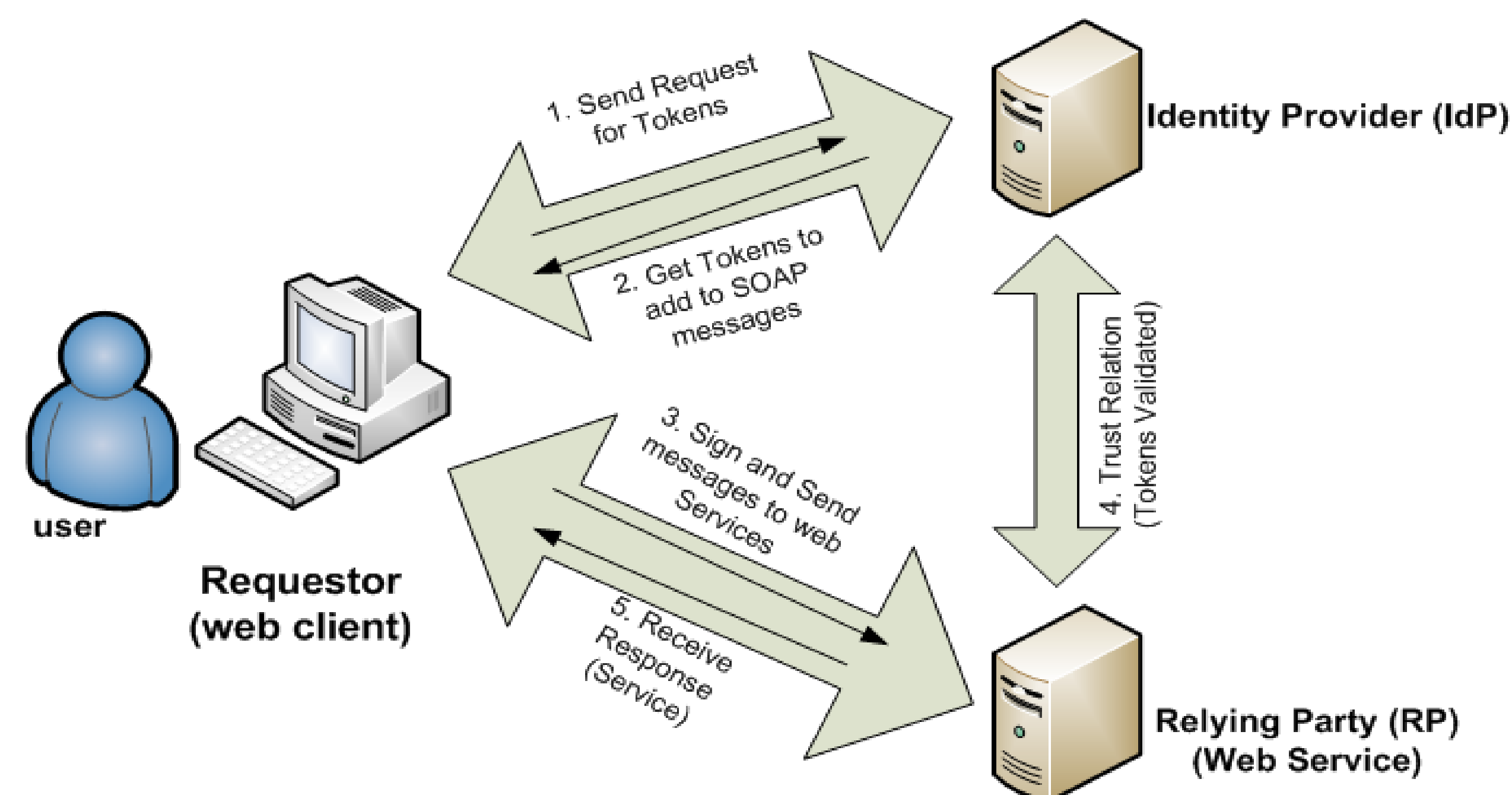


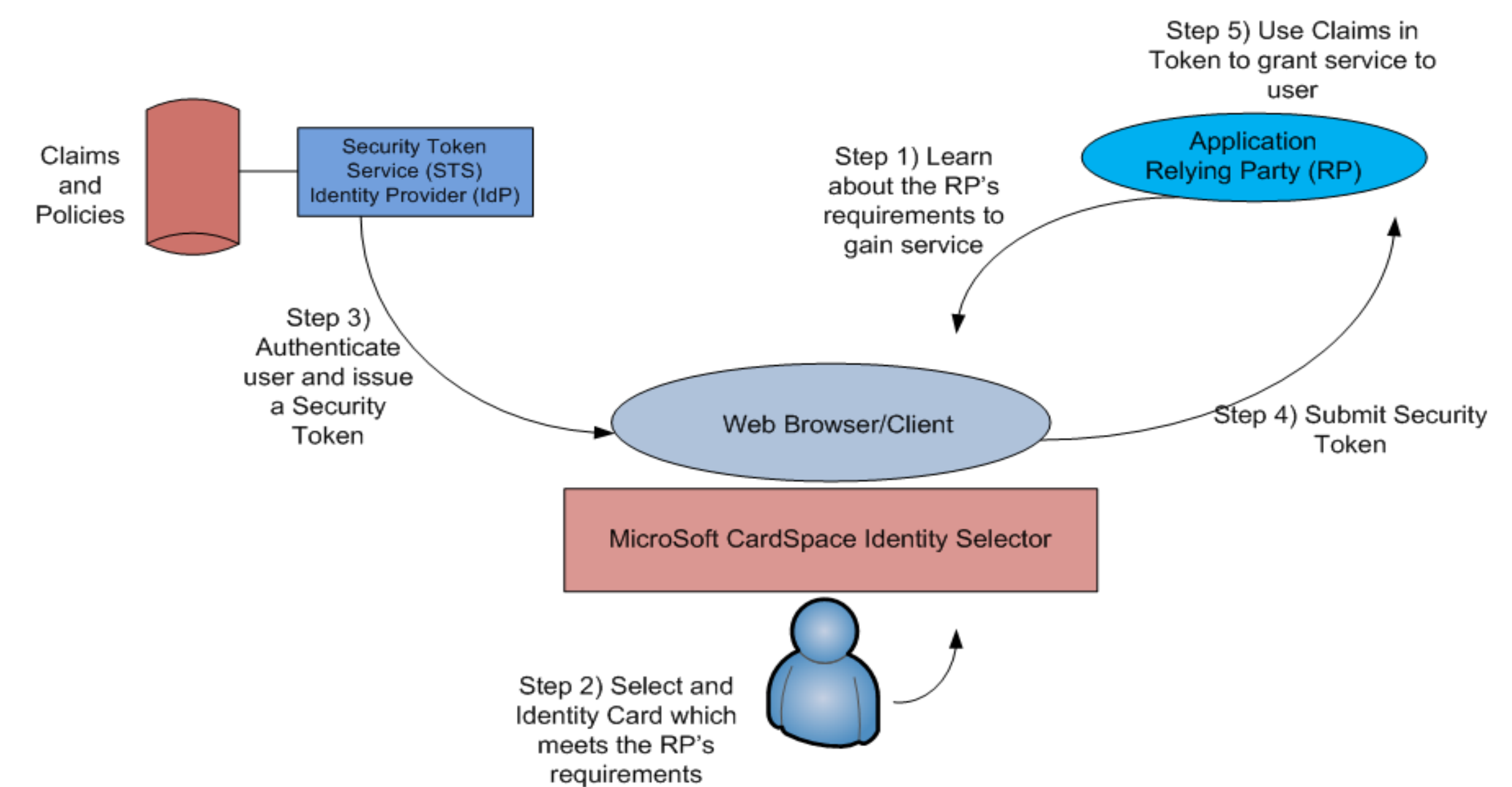
## Privacy Through Identity Management

Bharat Bhargava, Noopur Singh  
Purdue University

### WS- Federation Scenario (Direct Trust)



### CardSpace Model of Identity Management



### Issues With CardSpace

- RPs without any certificates at all can be used in the CardSpace framework (given user consent).
- Single Layer of authentication of the user by the IdP. User's privacy compromised if a working session is hijacked or the password is cracked.

### Privacy Preserving Methods

- Advanced cryptographic mechanism such as zero knowledge proofs.
- Predicates over attributes (type, value).
- Anonymous Credential (pseudonymous identification).

## Proposed Solution

Use of SAML assertions in SOAP messages, to include ZPK, predicates and Anonymous Credential.

