Privacy and Identity Management in Cloud

Rohit Ranchal, Bharat Bhargava, Pelin Angin, Noopur Singh,
Lotfi Ben Othmane, Leszek Lilien

Department of Computer Science
Purdue University, Western Michigan University
{rranchal, bbshail}@purdue.edu, leszek.lilien@wmich.edu

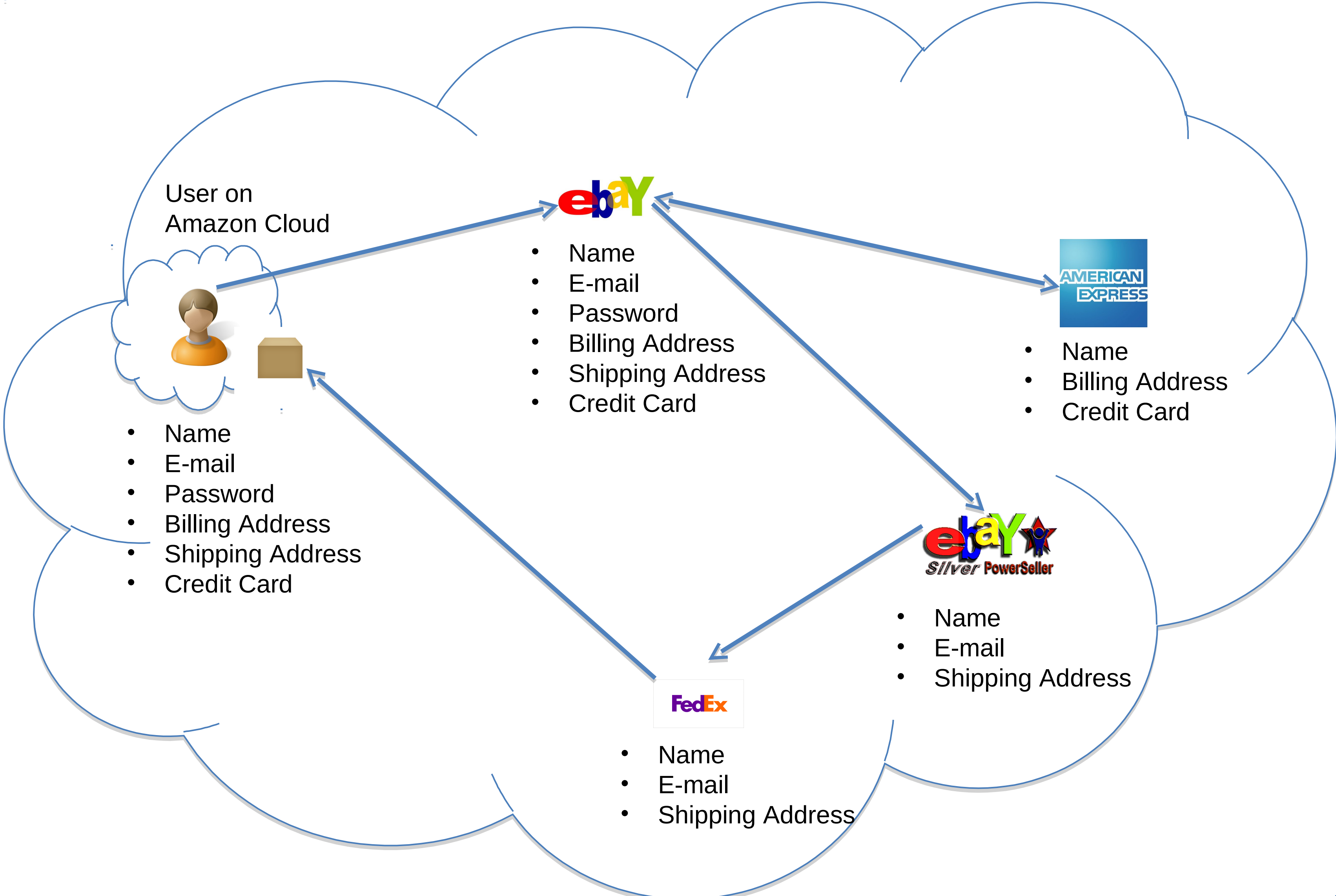
Mark Linderman
mark.linderman@rl.af.mil
Air Force Research Laboratory
Rome, NY, USA

This research was supported by AFRL Rome, USA and NGC

Outline

- **Motivation**
- **Identity Management (IDM)**
- **Goals of Proposed User-Centric IDM**
- **Mechanisms**
- **Description of proposed solution**
- **Advantages of the Proposed Scheme**
- **Conclusion & Future Work**
- **References**
- **Questions?**

Motivation



User on
Amazon Cloud

- Name
- E-mail
- Password
- Billing Address
- Shipping Address
- Credit Card

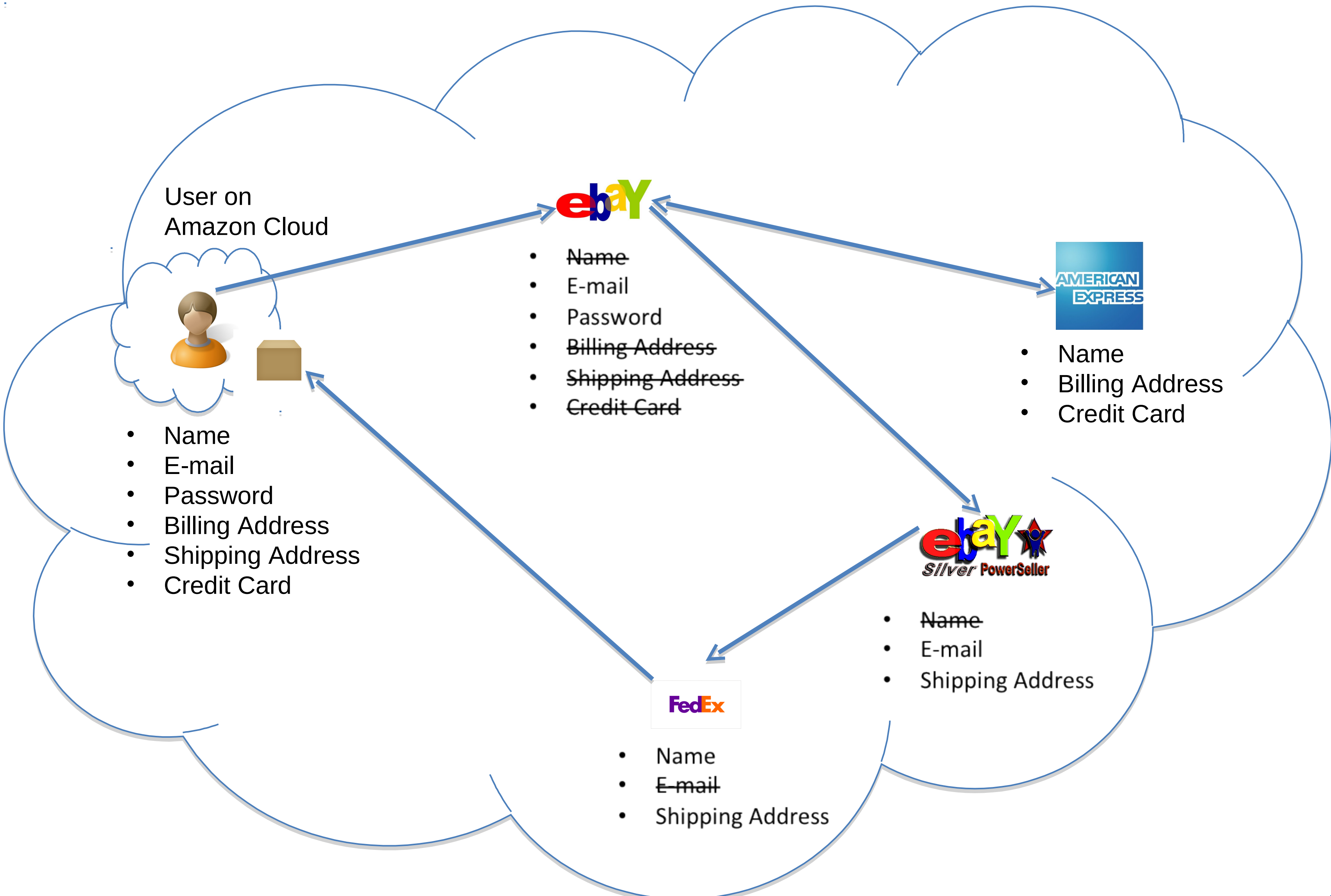
- Name
- E-mail
- Password
- Billing Address
- Shipping Address
- Credit Card

- Name
- Billing Address
- Credit Card

- Name
- E-mail
- Shipping Address

- Name
- E-mail
- Shipping Address

Motivation



User on
Amazon Cloud

- Name
- E-mail
- Password
- Billing Address
- Shipping Address
- Credit Card

- ~~Name~~
- E-mail
- Password
- ~~Billing Address~~
- ~~Shipping Address~~
- ~~Credit Card~~

- Name
- Billing Address
- Credit Card

- ~~Name~~
- E-mail
- Shipping Address

- Name
- ~~E-mail~~
- Shipping Address

Identity Management (IDM)

- **IDM in traditional application-centric IDM model**
  - Each service keeps track of identifying information of its users.
- **Existing IDM Systems**
  - Microsoft Windows CardSpace [W. A. Alrodhan]
  - OpenID [http://openid.net]
  - PRIME [S. F. Hubner, Karlstad Univ]

These systems require a trusted third party and do not work on an untrusted host.

If Trusted Third Party is compromised, all the identifying information
of the users is also compromised leading to serious problems like
Identity Theft.

[Latest: AT&T iPad leak]

IDM in Cloud Computing

- **Cloud introduces several issues to IDM**
  - Collusion between Cloud Services
    - **Users have multiple accounts associated with multiple service providers.**
    - **Sharing sensitive identity information between services can lead to undesirable mapping of the identities to the user.**
  - Lack of trust
    - **Cloud hosts are untrusted**
    - **Use of Trusted Third Party is not an option**
  - Loss of control
    - **Service-centric IDM Model**

IDM in Cloud needs to be user-centric

Goals of Proposed User-Centric IDM for the Cloud

1. **Authenticate without disclosing identifying information**
2. **Ability to securely use a service while on an untrusted host (VM on the cloud)**
3. **Minimal disclosure and minimized risk of disclosure during communication between user and service provider (Man in the Middle, Side Channel and Correlation Attacks)**
4. **Independence of Trusted Third Party for identity information**

Mechanisms in Proposed IDM

- **Active Bundle [L. Othmane, R. Ranchal]**
- **Anonymous Identification [A. Shamir]**
- **Computing Predicates with encrypted data [E. Shi]**
- **Multi-Party Computing [A. Shamir]**
- **Selective Disclosure [B. Laurie]**

Active Bundle

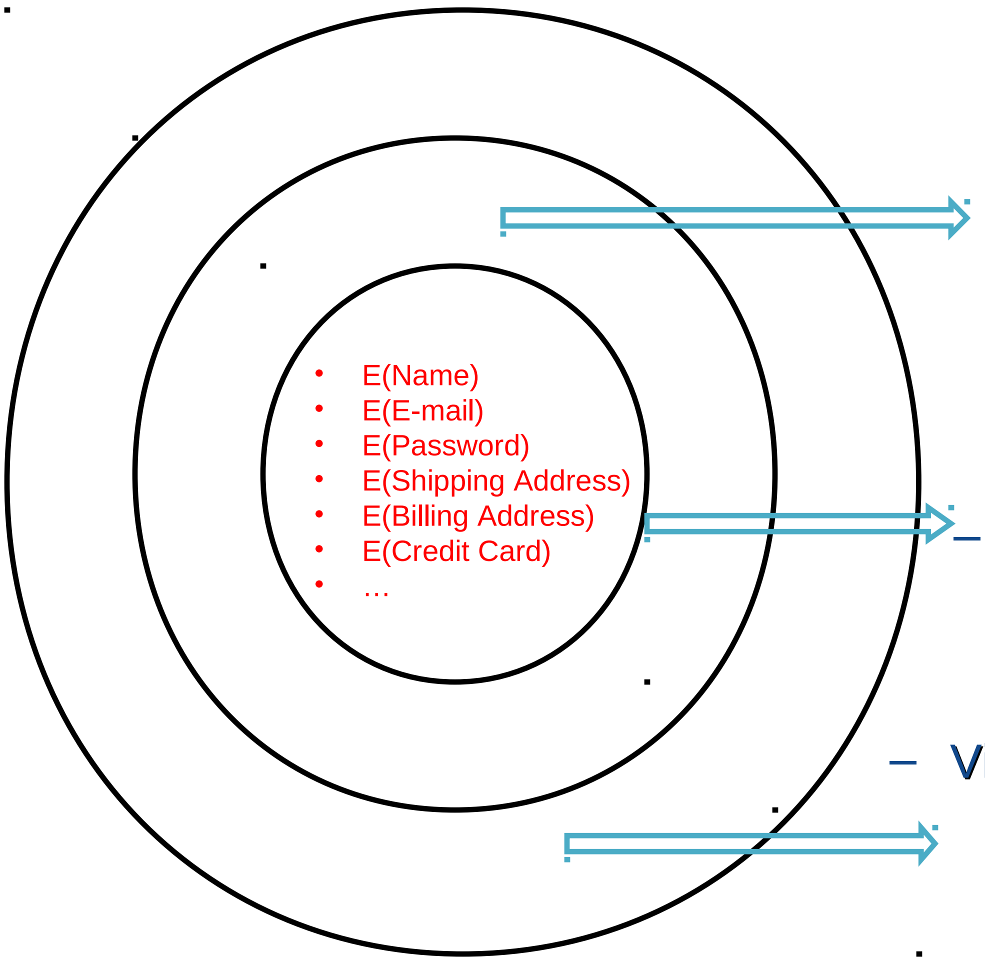
- **Active bundle (AB)**
  - An encapsulating mechanism protecting data carried within it
  - Includes data
  - Includes metadata used for managing confidentiality
    - **Both privacy of data and privacy of the whole AB**
  - Includes Virtual Machine (VM)
    - **performing a set of operations**
    - **protecting its confidentiality**
- **Active Bundles—Operations**
  - Self-Integrity check

    E.g., Uses a hash function
  - Evaporation/ Filtering

    Self-destroys (a part of) AB’s sensitive data when threatened with a disclosure
  - Apoptosis

    Self-destructs AB’s completely

Active Bundle Scheme



- E(Name)
- E(E-mail)
- E(Password)
- E(Shipping Address)
- E(Billing Address)
- E(Credit Card)
- …

– Metadata:
  - Access control policies
  - Data integrity checks
  - Dissemination policies
  - Life duration
  - ID of a trust server
  - ID of a security server
  - App-dependent information
  - …

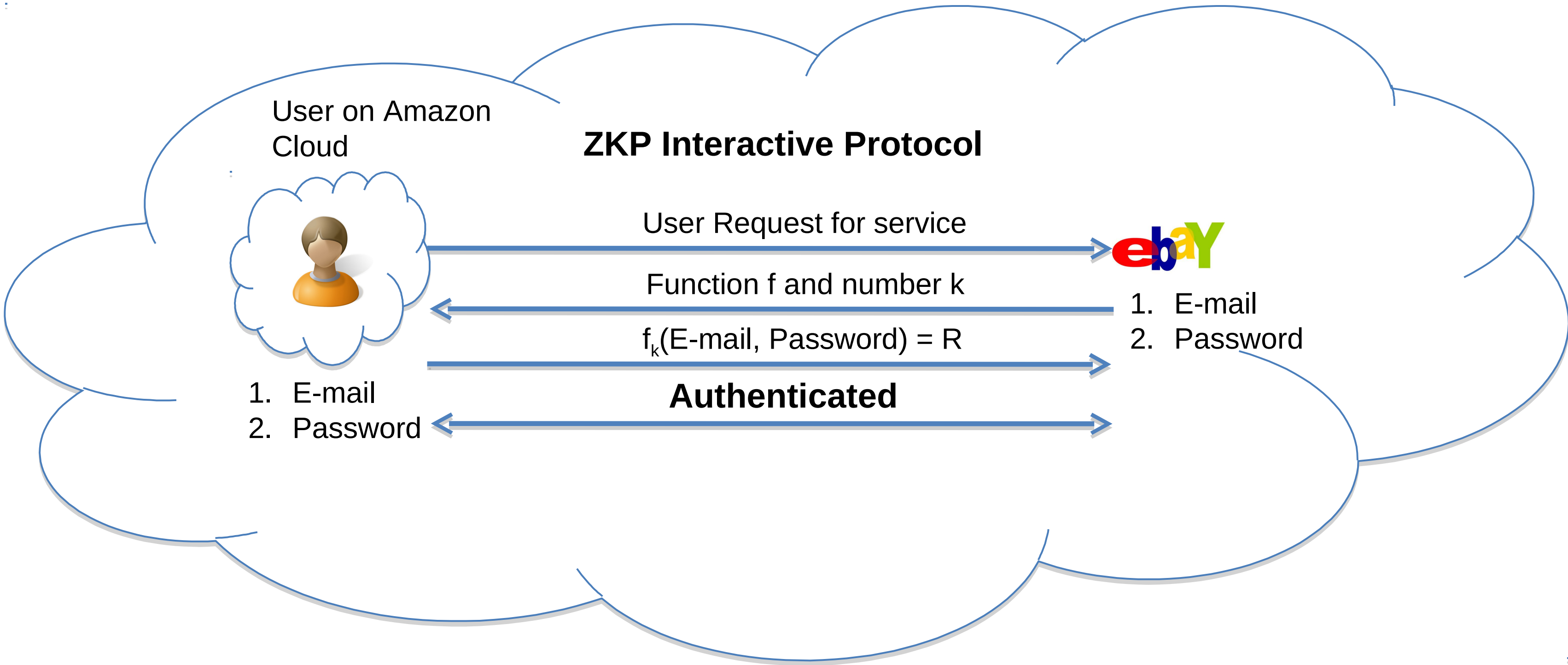
– Sensitive Data:
  - Identity Information
  - ...

– Virtual Machine (algorithm):
  - Interprets metadata
  - Checks active bundle integrity
  - Enforces access and dissemination control policies
  - …

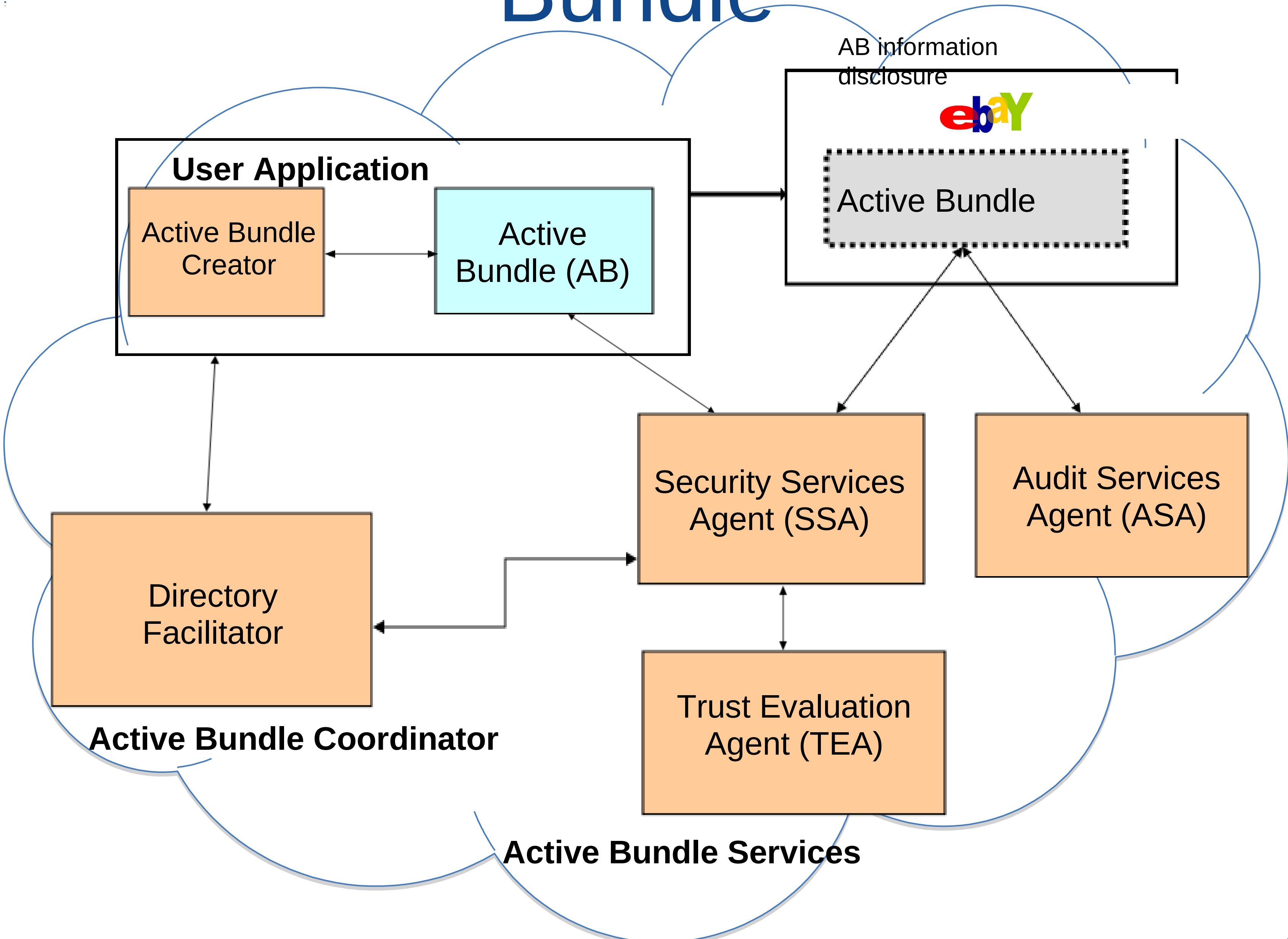
*** E( ) - Encrypted Information**

Anonymous Identification

- Use of Zero-knowledge proofing for user authentication without disclosing its identifier.



Interaction using Active Bundle



User Application

Active Bundle Creator

Active Bundle (AB)

AB information disclosure

Active Bundle

Directory Facilitator

Active Bundle Coordinator

Security Services Agent (SSA)

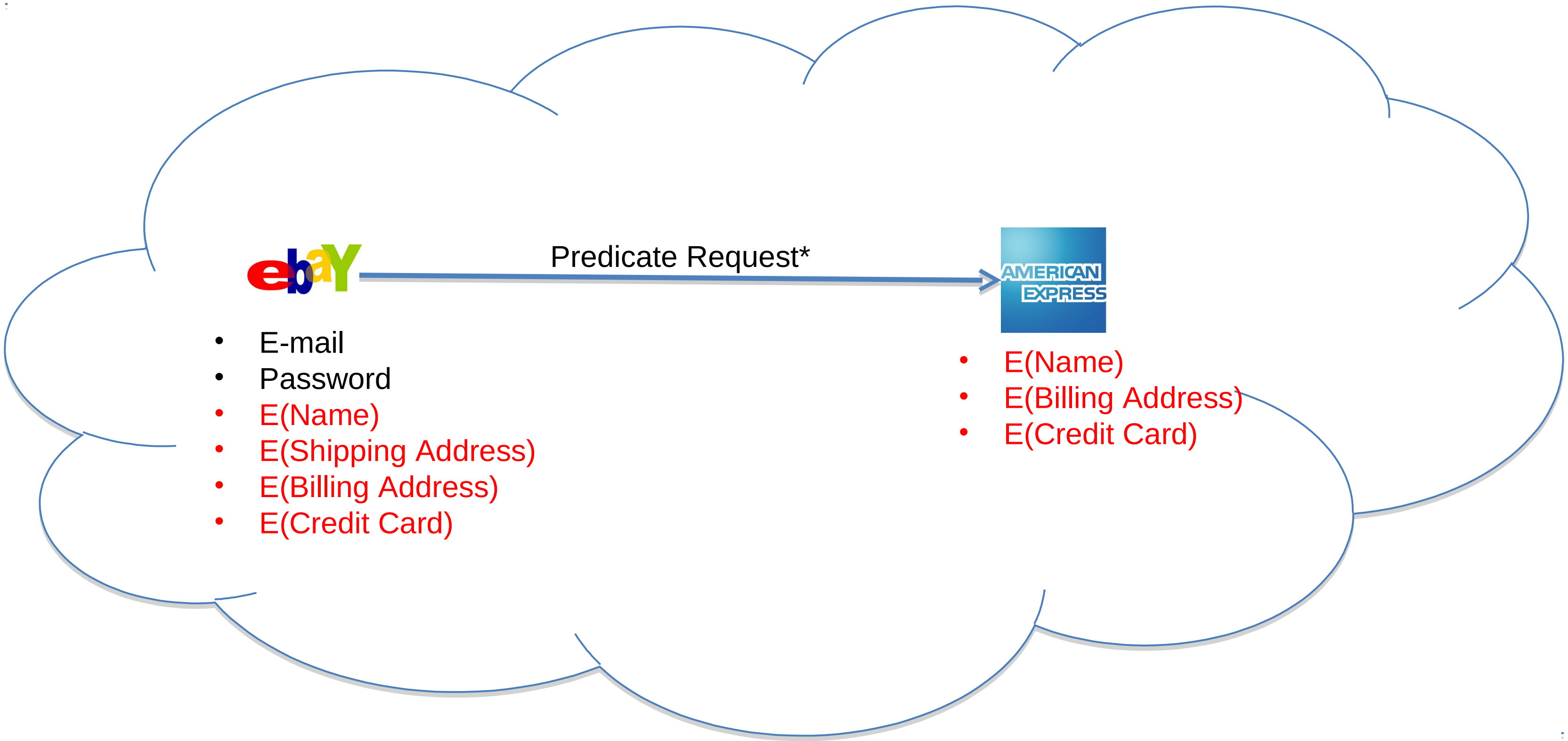
Audit Services Agent (ASA)

Trust Evaluation Agent (TEA)

Active Bundle Services

Predicate over Encrypted Data

- Verification without disclosing unencrypted identity data.



Predicate Request*

- E-mail
- Password
- E(Name)
- E(Shipping Address)
- E(Billing Address)
- E(Credit Card)

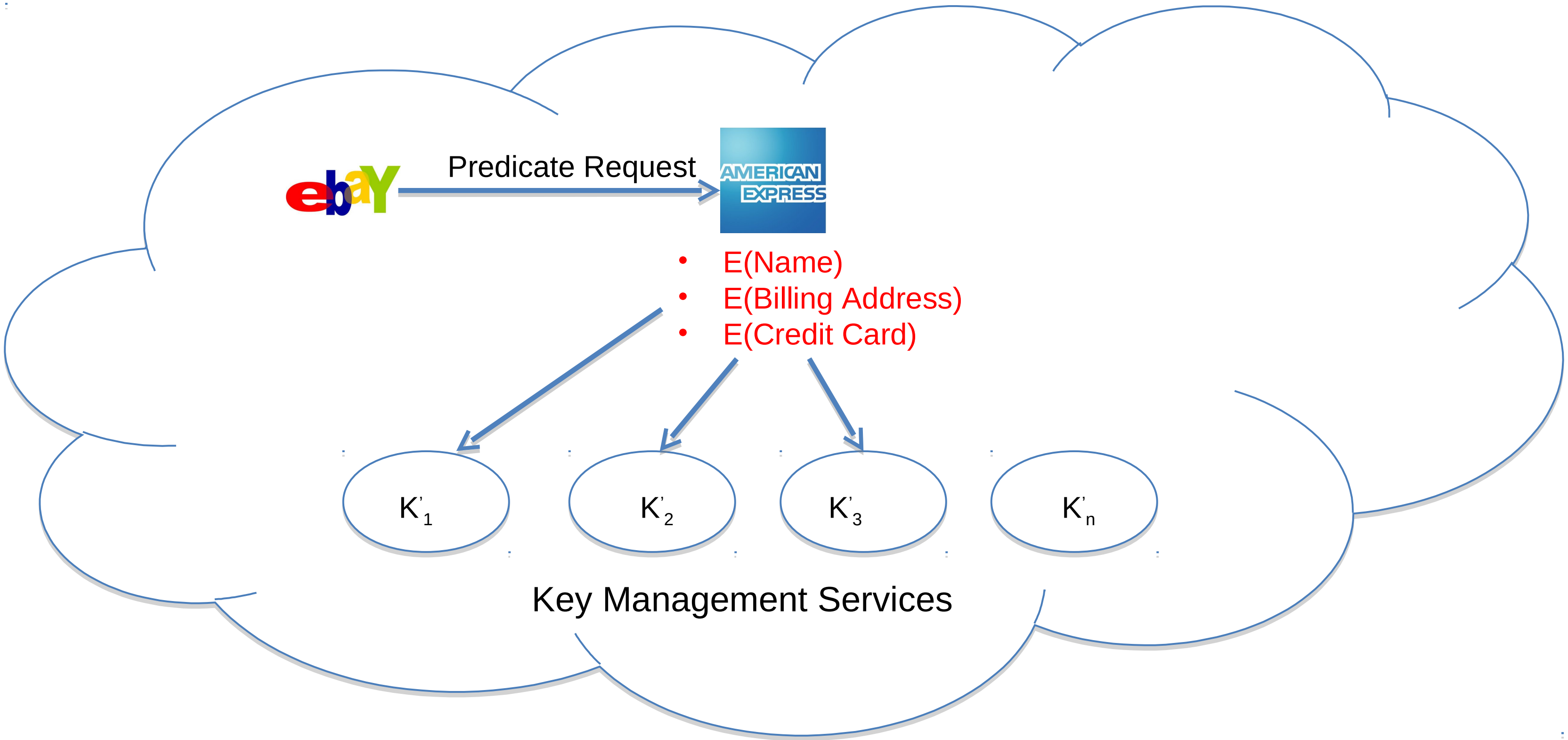
- E(Name)
- E(Billing Address)
- E(Credit Card)

*Age Verification Request

*Credit Card Verification Request

Multi-Party Computing

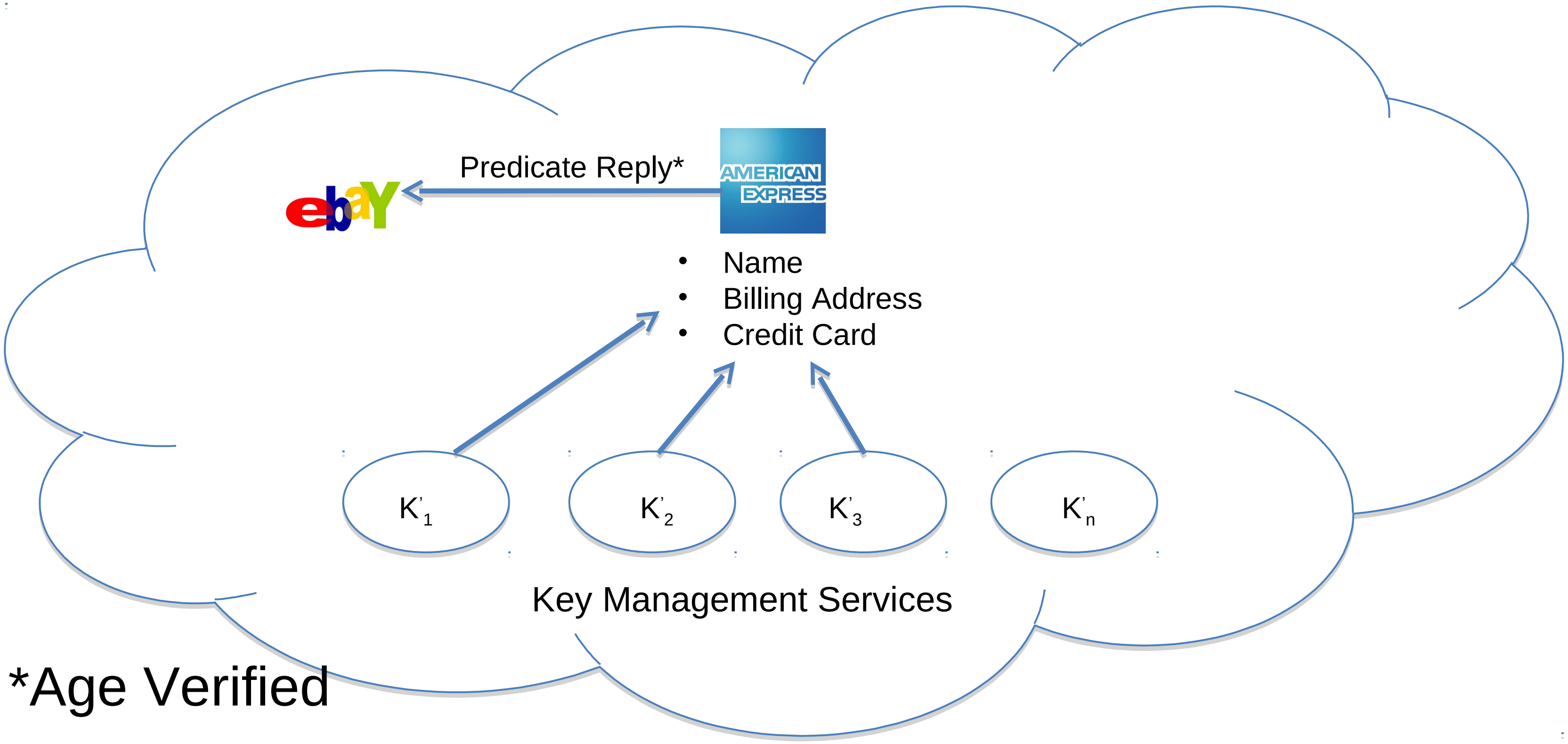
- To become independent of a trusted third party
  - Multiple Services hold shares of the secret key
  - Minimize the risk



* Decryption of information is handled by the Key Management services

Multi-Party Computing

- To become independent of a trusted third party
  - Multiple Services hold shares of the secret key
  - Minimize the risk



- Name
- Billing Address
- Credit Card

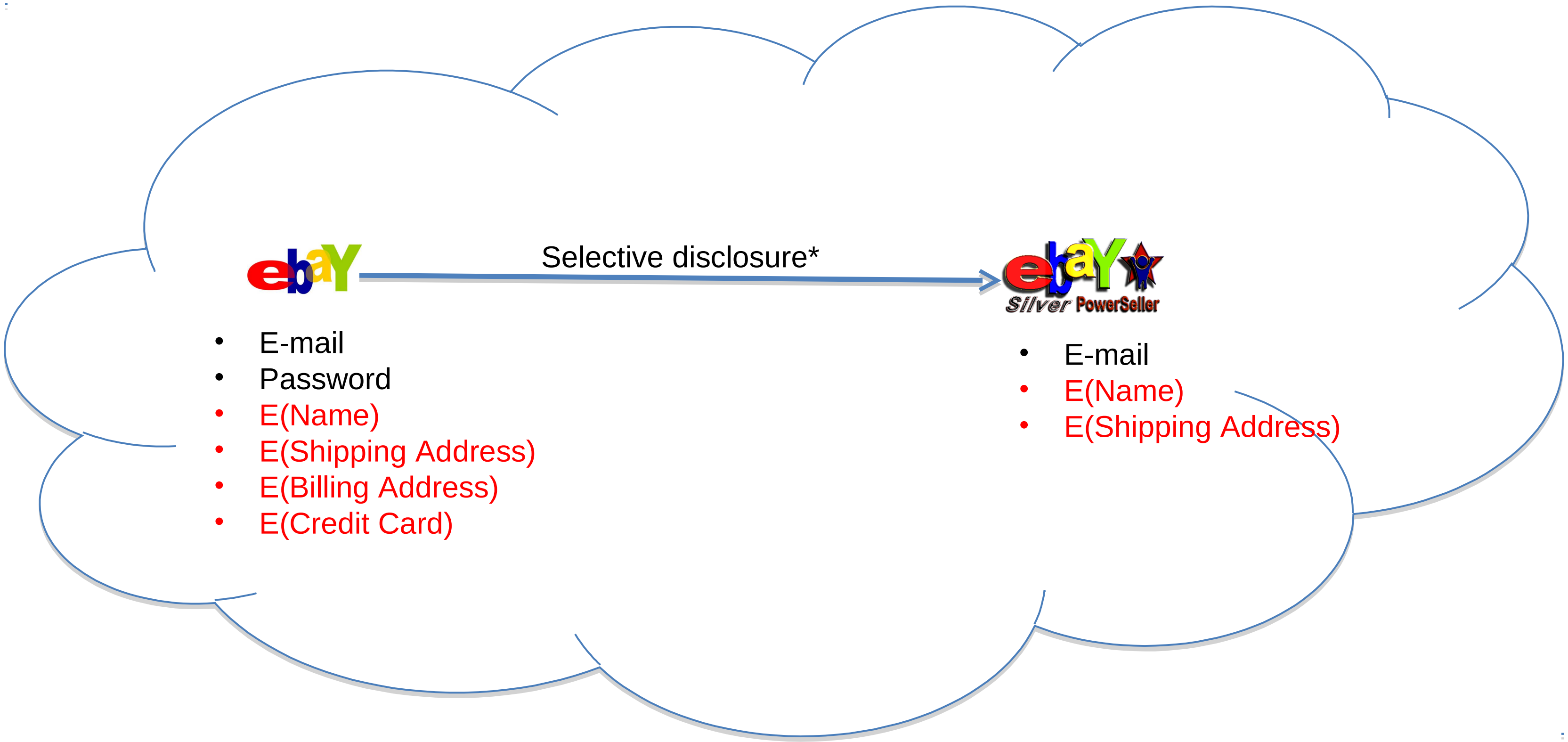
Key Management Services

*Age Verified

*Credit Card Verified

Selective Disclosure

- User Policies in the Active Bundle dictate dissemination



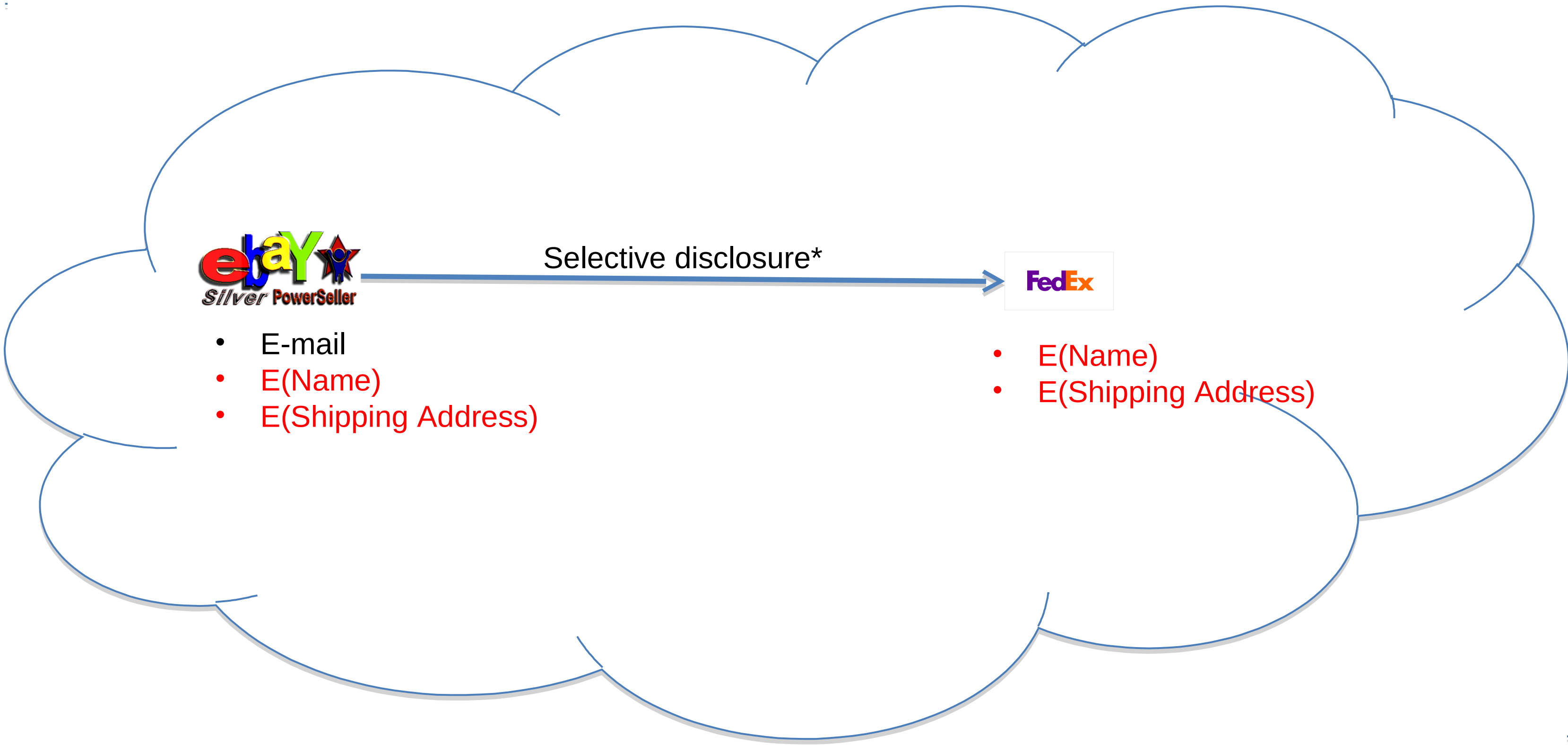
Selective disclosure*

- E-mail
- Password
- E(Name)
- E(Shipping Address)
- E(Billing Address)
- E(Credit Card)

- E-mail
- E(Name)
- E(Shipping Address)

*e-bay shares the encrypted information based on the user policy

Selective Disclosure



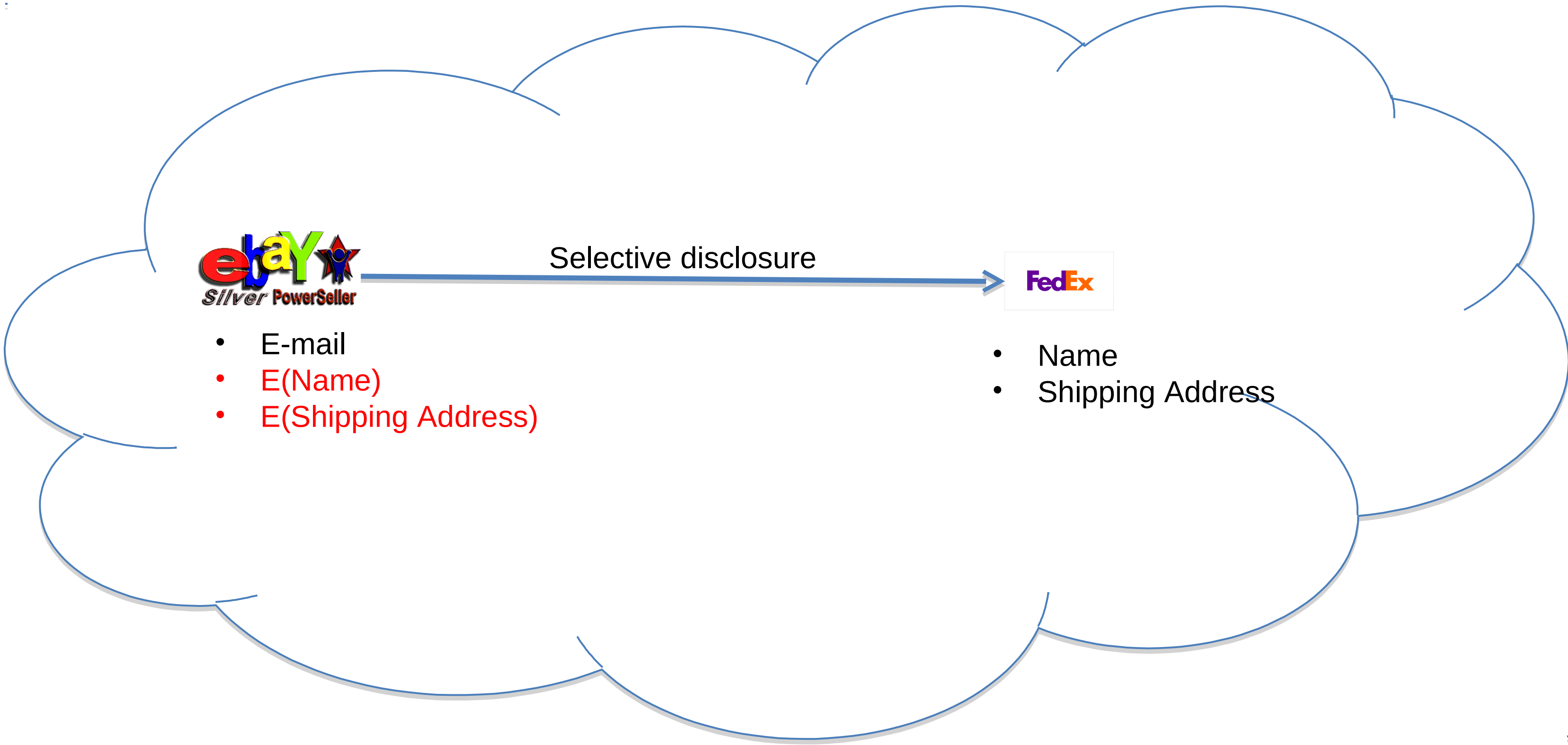
Selective disclosure*

- E-mail
- E(Name)
- E(Shipping Address)

- E(Name)
- E(Shipping Address)

*e-bay seller shares the encrypted information based on the user policy

Selective Disclosure



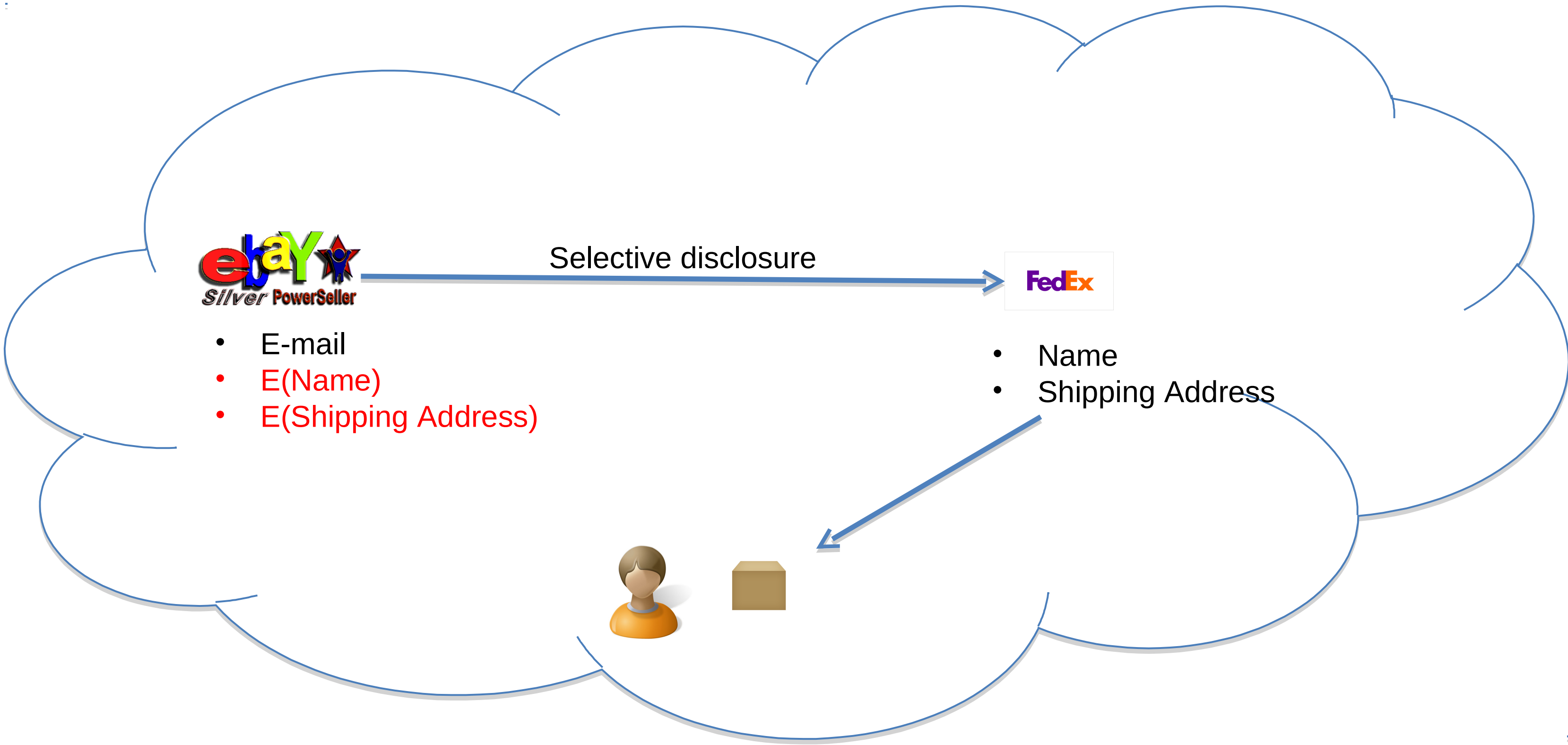
Selective disclosure

- E-mail
- E(Name)
- E(Shipping Address)

- Name
- Shipping Address

- Decryption handled by Multi-Party Computing as in the previous slides

Selective Disclosure



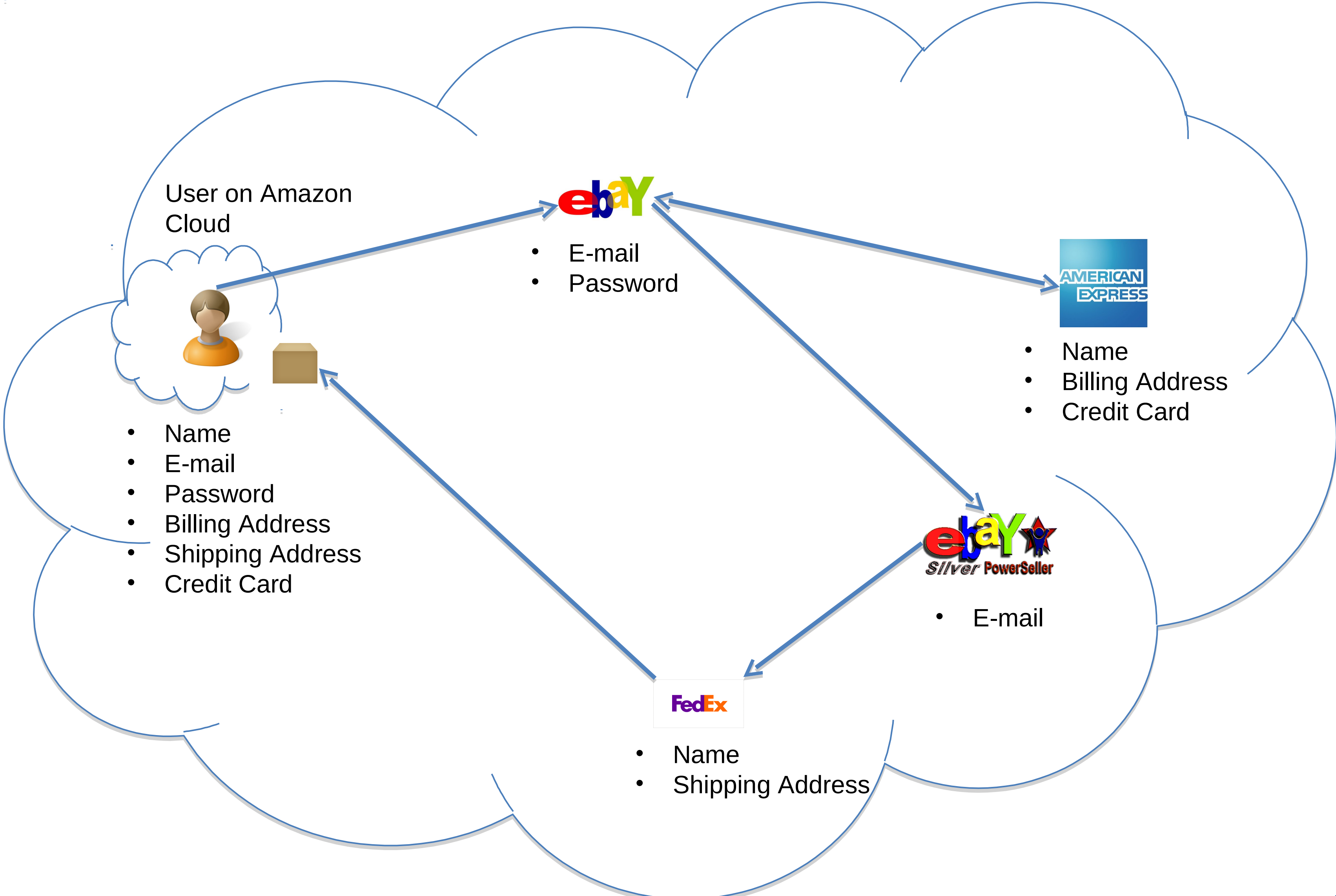
Selective disclosure

- E-mail
- E(Name)
- E(Shipping Address)

- Name
- Shipping Address

- Fed-Ex can now send the package to the user

Identity in the Cloud



User on Amazon Cloud

- Name
- E-mail
- Password
- Billing Address
- Shipping Address
- Credit Card

- E-mail
- Password

- Name
- Billing Address
- Credit Card

- E-mail

- Name
- Shipping Address

Characteristics and Advantages

- **Ability to use Identity data on untrusted hosts**
  - Self Integrity Check

  - Integrity compromised- apoptosis or evaporation
  - Data should not be on this host
- **Establishes the trust of users in IDM**
  - Through putting the user in control of who has his data and how is is used
  - Identity is being used in the process of authentication, negotiation, and data exchange.
- **Independent of Third Party for Identity Information**
  - Minimizes correlation attacks
- **Minimal disclosure to the SP**
  - SP receives only necessary information.

Conclusion & Future Work

- **Problems with IDM in Cloud Computing**
  - Collusion of Identity Information
  - Prohibited Untrusted Hosts
  - Usage of Trusted Third Party
- **Proposed Approaches**
  - IDM based on Anonymous Identification
  - IDM based on Predicate over Encrypted data
  - IDM based on Multi-Party Computing
- **Future work**
  - Develop the prototype, conduct experiments and evaluate the approach

References

[1] C. Sample and D. Kelley. *Cloud Computing Security: Routing and DNS Threats*, http://www.securitycurve.com/wordpress/, June 23,2009.

[2] W. A. Alrodhan and C. J. Mitchell. *Improving the Security of CardSpace*, EURASIP Journal on Information Security Vol. 2009, doi:10.1155/2009/167216, 2009.

[3] OPENID, http://openid.net/, 2010.

[4] S. F. Hubner. HCI work in PRIME, https://www.prime-project.eu/, 2008.

[5] A. Gopalakrishnan, *Cloud Computing Identity Management*, SETLabsBriefings, Vol7, http://www.infosys.com/research/, 2009.

[6] A. Barth, A. Datta, J. Mitchell and H. Nissenbaum. *Privacy and Contextual Integrity: Framework and Applications*, Proc. of the 2006 IEEE Symposium on Security and Privacy, 184-198.

[7] L. Othmane, *Active Bundles for Protecting Confidentiality of Sensitive Data throughout Their Lifecycle,* PhD Thesis, Western Michigan Univ, 2010.

[8] A. Fiat and A. Shamir, *How to prove yourself: Practical Solutions to Identification and Signature Problems,* CRYPTO, 1986.

[9] A. Shamir, *How to Share a Secret,* Communications of the ACM, 1979.

[10] M. Ben-Or, S. Goldwasser and A. Wigderson, *Completeness theorems for non-cryptographic fault-tolerant distributed computation*, ACM Symposium on Theory of Computing, 1988.

[11] E. Shi, *Evaluating Predicates over Encrypted Data*, PhD Thesis, CMU, 2008.