Cloud Security and Privacy

- POLICY LANGUAGE
- CERTIFICATION

Minimize Lack of Trust

Minimize Lack of Trust: Policy Language

- Consumers have specific security needs but don't have a say-so in how they are handled
  - What the heck is the provider doing for me?
  - Currently consumers cannot dictate their requirements to the provider (SLAs are one-sided)
- Standard language to convey one's policies and expectations
  - Agreed upon and upheld by both parties
  - Standard language for representing SLAs
  - Can be used in a intra-cloud environment to realize overarching security posture

Minimize Lack of Trust: Policy Language (Cont.)

- Create policy language with the following characteristics:
  - Machine-understandable (or at least processable),
  - Easy to combine/merge and compare
  - Examples of policy statements are, “requires isolation between VMs”, “requires geographical isolation between VMs”, “requires physical separation between other communities/tenants that are in the same industry,” etc.
  - Need a validation tool to check that the policy created in the standard language correctly reflects the policy creator’s intentions (i.e. that the policy language is semantically equivalent to the user’s intentions).

Minimize Lack of Trust: Certification

- Certification
  - Some form of reputable, independent, comparable assessment and description of security features and assurance
  - Sarbanes-Oxley, DIACAP, DISTCAP, etc (are they sufficient for a cloud environment?)
- Risk assessment
  - Performed by certified third parties
  - Provides consumers with additional assurance

Minimize Loss of Control

- MONITORING
- UTILIZING DIFFERENT CLOUDS
- ACCESS CONTROL MANAGEMENT
- IDENTITY MANAGEMENT (IDM)

Minimize Loss of Control: Monitoring

- Cloud consumer needs situational awareness for critical applications
  - When underlying components fail, what is the effect of the failure to the mission logic
  - What recovery measures can be taken (by provider and consumer)
- Requires an application-specific run-time monitoring and management tool for the consumer
  - The cloud consumer and cloud provider have different views of the system
  - Enable both the provider and tenants to monitor the components in the cloud that are under their control

Minimize Loss of Control: Monitoring (Cont.)

- Provide mechanisms that enable the provider to act on attacks he can handle.
  - infrastructure remapping (create new or move existing fault domains)
  - shutting down offending components or targets (and assisting tenants with porting if necessary
  - Repairs
- Provide mechanisms that enable the consumer to act on attacks that he can handle (application-level monitoring).
  - RAdAC (Risk-adaptable Access Control)
  - VM porting with remote attestation of target physical host
  - Provide ability to move the user's application to another cloud

Minimize Loss of Control: Utilize Different Clouds

- The concept of ‘Don’t put all your eggs in one basket’
  - Consumer may use services from different clouds through an intra-cloud or multi-cloud architecture
  - Propose a multi-cloud or intra-cloud architecture in which consumers
    - Spread the risk
    - Increase redundancy (per-task or per-application)
    - Increase chance of mission completion for critical applications
  - Possible issues to consider:
    - Policy incompatibility (combined, what is the overarching policy?)
    - Data dependency between clouds
    - Differing data semantics across clouds
    - Knowing when to utilize the redundancy feature (monitoring technology)
    - Is it worth it to spread your sensitive data across multiple clouds?
      - Redundancy could increase risk of exposure

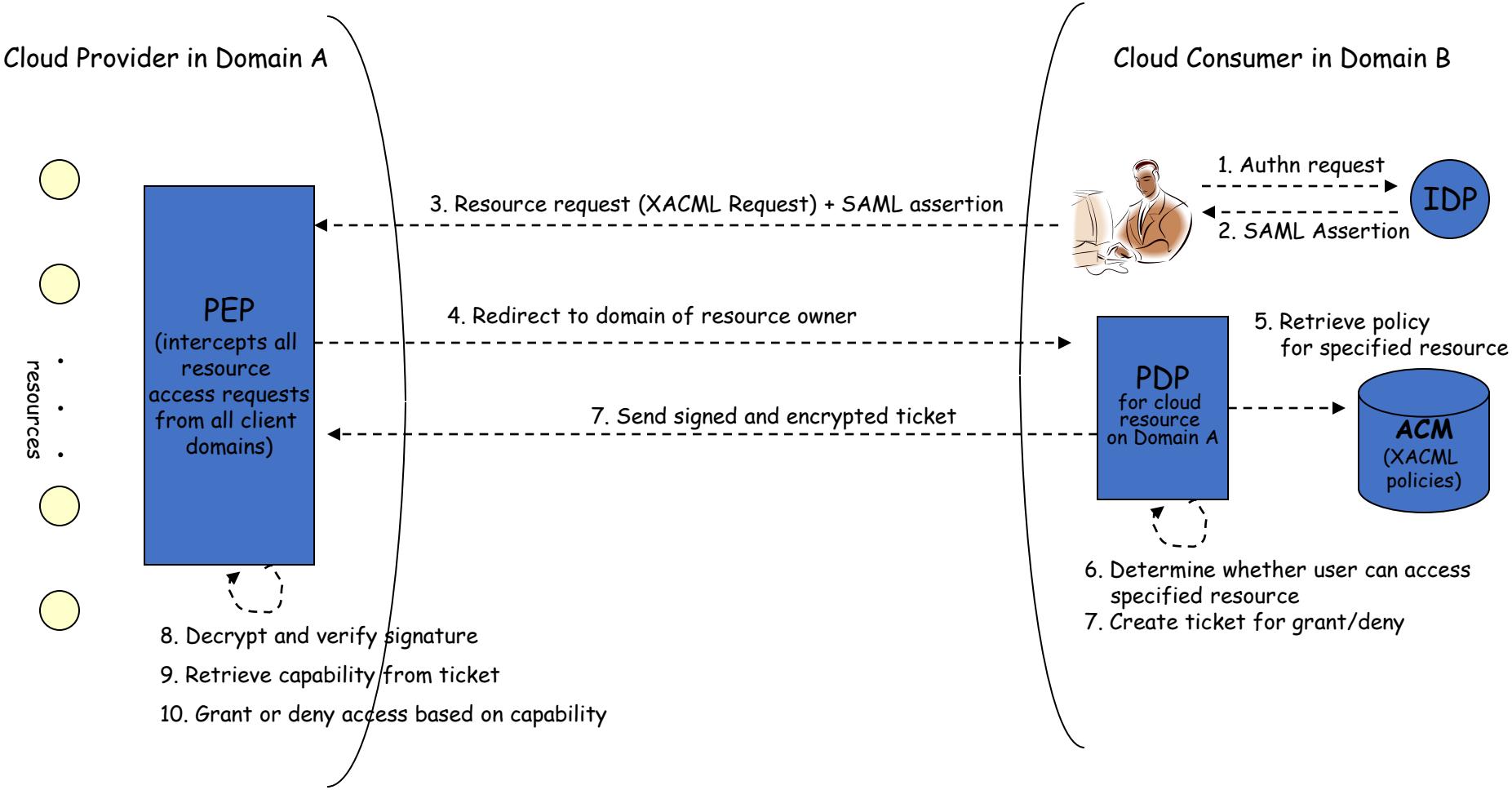
Minimize Loss of Control: Access Control

- Many possible layers of access control
  - E.g. access to the cloud, access to servers, access to services, access to databases (direct and queries via web services), access to VMs, and access to objects within a VM
  - Depending on the deployment model used, some of these will be controlled by the provider and others by the consumer
- Regardless of deployment model, provider needs to manage the user authentication and access control procedures (to the cloud)
  - Federated Identity Management: access control management burden still lies with the provider
  - Requires user to place a large amount of trust on the provider in terms of security, management, and maintenance of access control policies. This can be burdensome when numerous users from different organizations with different access control policies, are involved

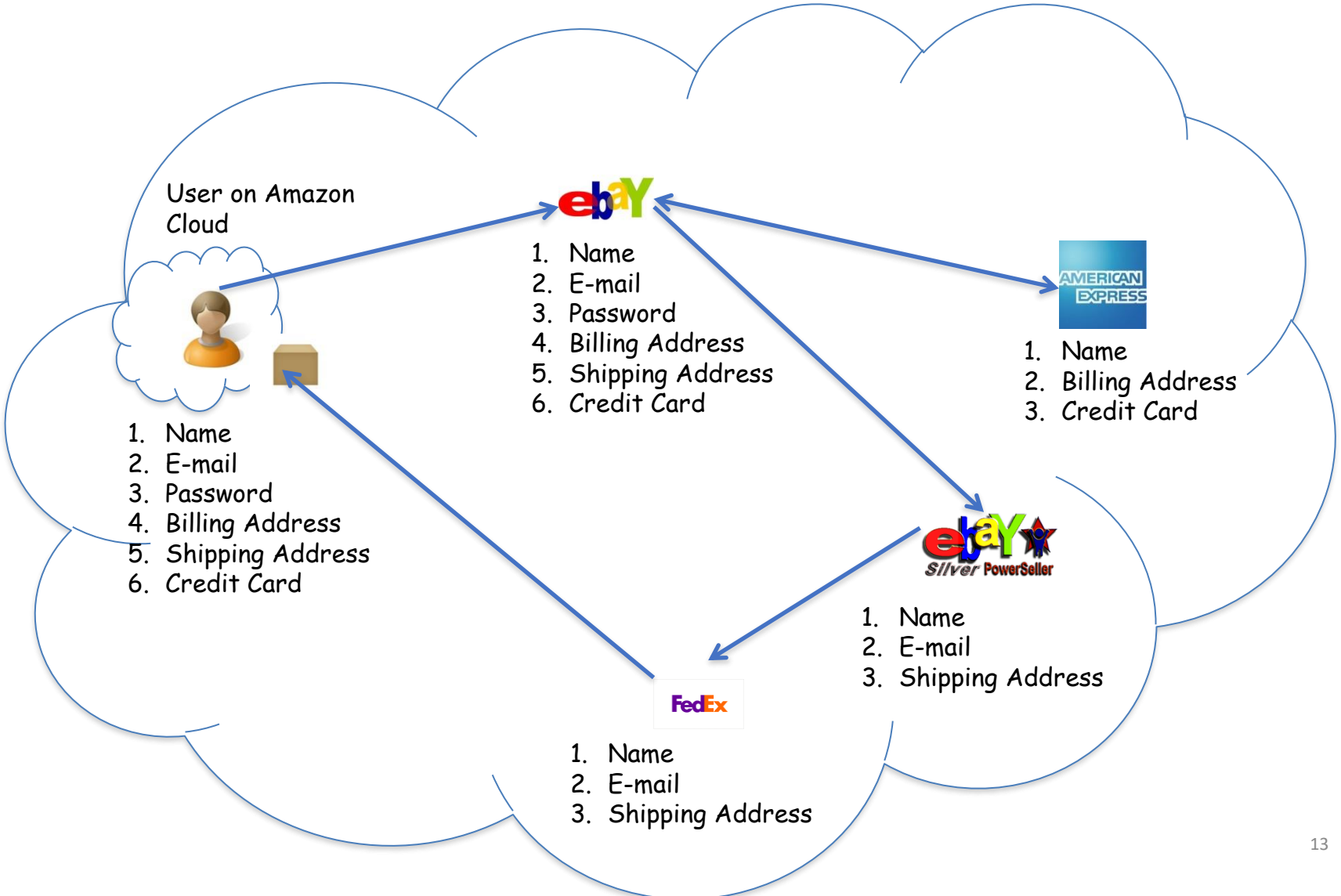
Minimize Loss of Control: Access Control (Cont.)

- Consumer-managed access control
  - Consumer retains decision-making process to retain some control, requiring less trust of the provider (i.e. PDP is in consumer's domain)
  - Requires the client and provider to have a pre-existing trust relationship, as well as a pre-negotiated standard way of describing resources, users, and access decisions between the cloud provider and consumer. It also needs to be able to guarantee that the provider will uphold the consumer-side's access decisions.
  - Should be at least as secure as the traditional access control model.
  - Facebook and Google Apps do this to some degree, but not enough control
  - Applicability to privacy of patient health records

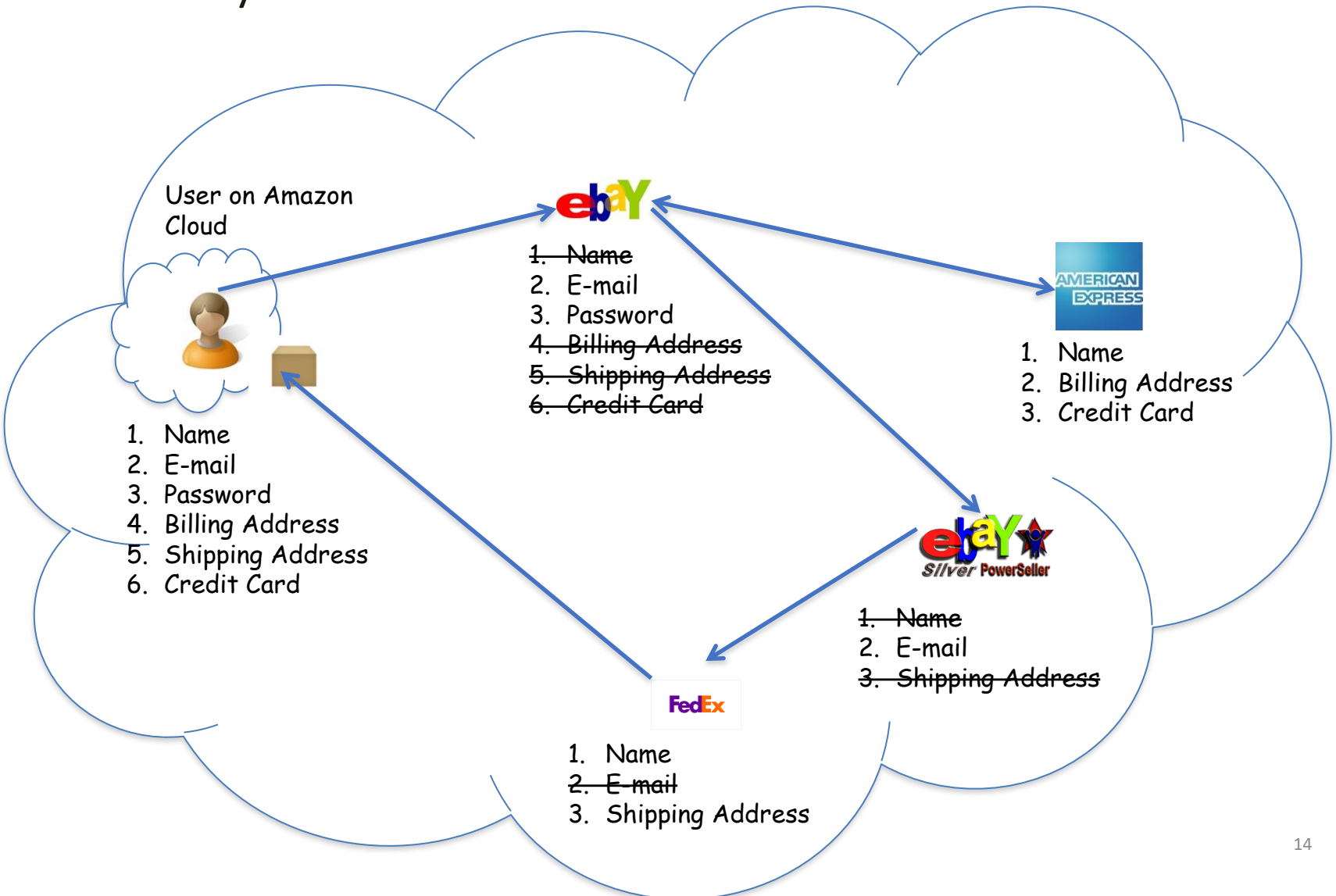
Minimize Loss of Control: Access Control



Minimize Loss of Control: IDM Motivation



Minimize Loss of Control: IDM Identity in the Cloud



Minimize Loss of Control: IDM
Present IDMs

- IDM in traditional application-centric IDM model
  - Each application 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]

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

[Latest: **AT&T iPad leak]**

Minimize Loss of Control: IDM Issues in Cloud Computing

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

IDM in Cloud needs to be user-centric

Minimize Loss of Control: IDM
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

Minimize Loss of Control: IDM Approach - 1

- **IDM Wallet:**
  - Use of AB scheme to protect PII from untrusted hosts.
- **Anonymous Identification:**
  - Use of Zero-knowledge proofing for authentication of an entity without disclosing its identifier.

Minimize Loss of Control: IDM Components of Active Bundle (Approach – 1)

- **Identity data:** Data used during authentication, getting service, using service (i.e. SSN, Date of Birth).
- **Disclosure policy:** A set of rules for choosing Identity data from a set of identities in IDM Wallet.
- **Disclosure history:** Used for logging and auditing purposes.
- **Negotiation policy:** This is Anonymous Identification, based on the Zero Knowledge Proofing.
- **Virtual Machine:** Code for protecting data on untrusted hosts. It enforces the disclosure policies.

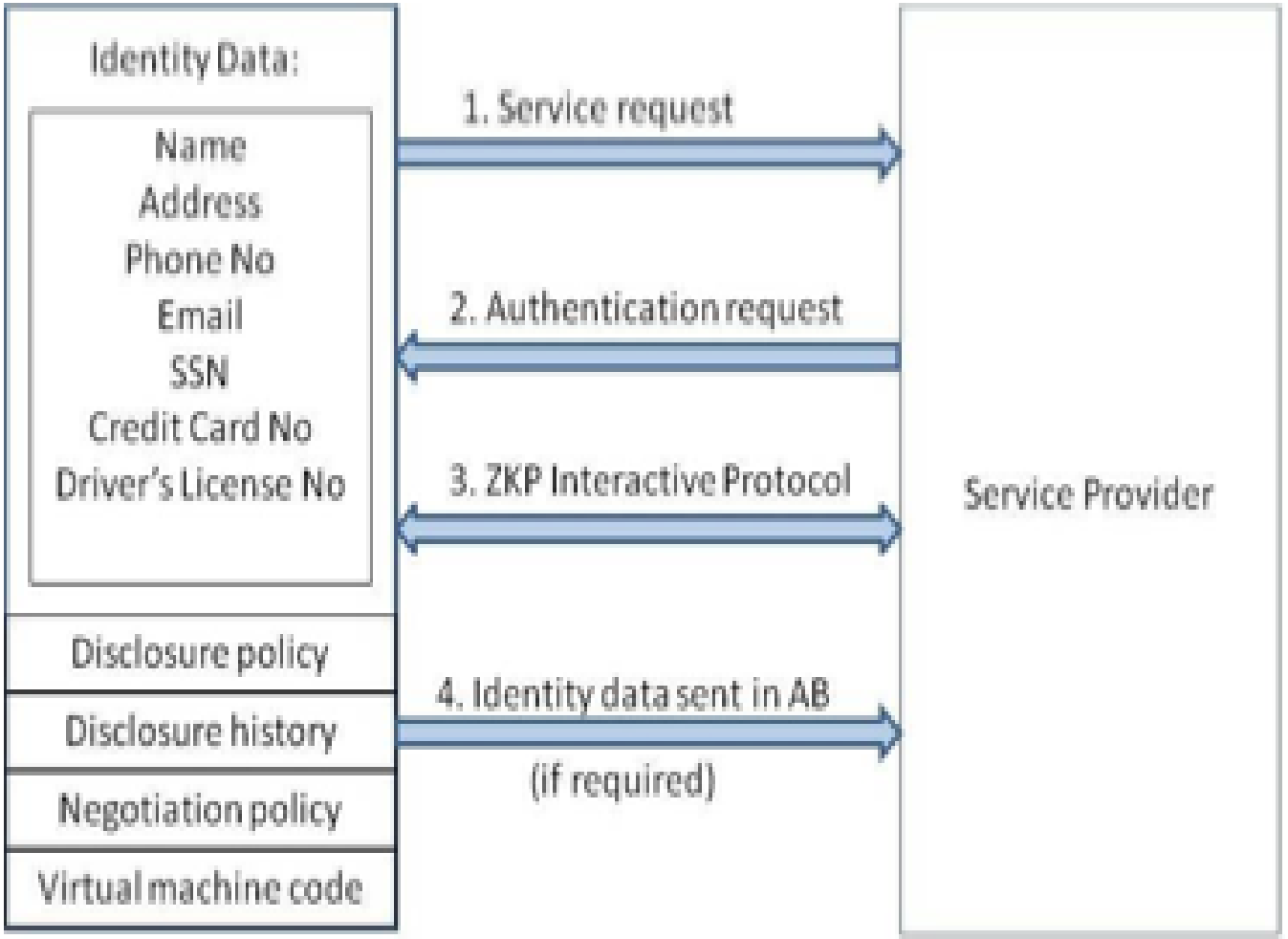
Minimize Loss of Control: IDM
Anonymous Identification (Approach – 1)

Anonymous Identification

(Shamir's approach for Credit Cards)

- IdP provides Encrypted Identity Information to the user and SP.
- SP and User interact
- Both run IdP's public function on the certain bits of the Encrypted data.
- Both exchange results and agree if it matches.

Minimize Loss of Control: IDM Usage Scenario (Approach – 1)



Minimize Loss of Control: IDM Approach - 2

- Active Bundle scheme to protect PII from untrusted hosts
- Predicates over encrypted data to authenticate without disclosing unencrypted identity data.
- Multi-party computing to be independent of a trusted third party

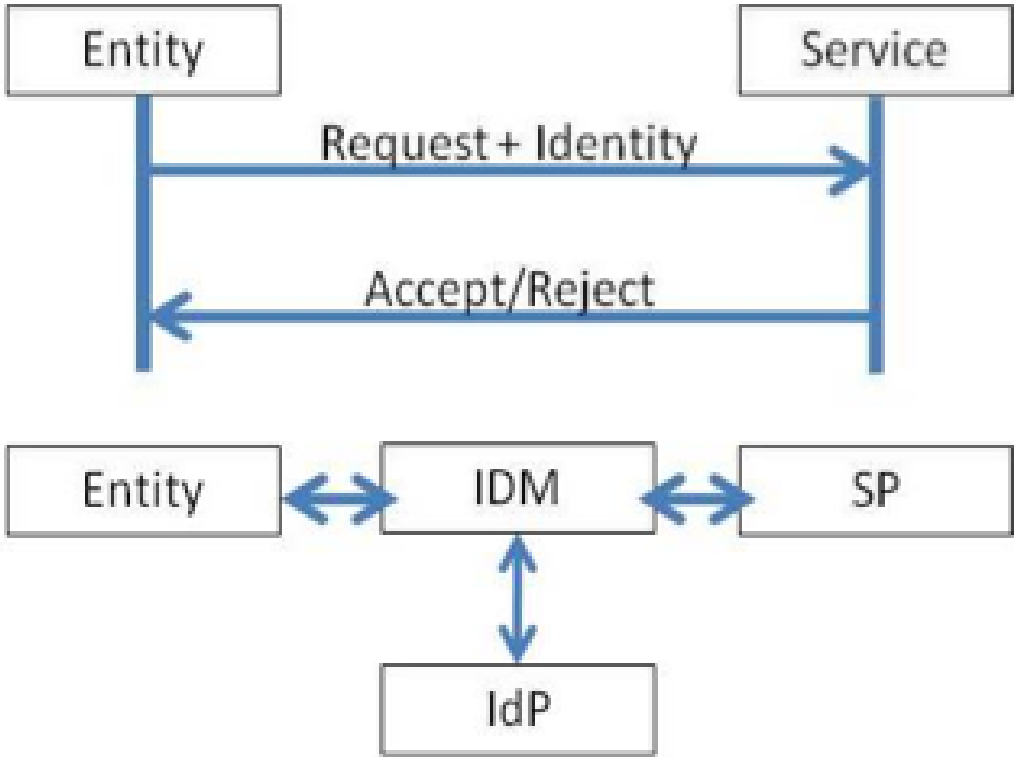
Minimize Loss of Control: IDM Usage Scenario (Approach – 2)

- Owner O encrypts Identity Data(PII) using algorithm Encrypt and O's public key PK. Encrypt outputs CT—the encrypted PII.
- SP transforms his request for PII to a predicate represented by function p.
- SP sends shares of p to the n parties who hold the shares of MSK.
- n parties execute together KeyGen using PK, MSK, and p, and return TKp to SP.
- SP calls the algorithm Query that takes as input PK, CT, TKp and produces p(PII) which is the evaluation of the predicate.
- The owner O is allowed to use the service only when the predicate evaluates to "true".

Minimize Loss of Control: IDM Representation of identity information for negotiation

- Token/Pseudonym
- Identity Information in clear plain text
- **Active Bundle**

Minimize Loss of Control: IDM Motivation-Authentication Process using PII



Problem: Which information to disclose and how to disclose it.

Proposed IDM: Mechanisms

- [16] *Protection of Identity Information in Cloud Computing without Trusted Third Party* - R. Ranchal, B. Bhargava, L.B. Othmane, L. Lilien, A. Kim, M. Kang, Third International Workshop on Dependable Network Computing and Mobile Systems (DNCMS) in conjunction with 29th IEEE Symposium on Reliable Distributed System (SRDS) 2010
- [17] *A User-Centric Approach for Privacy and Identity Management in Cloud Computing* - P. Angin, B. Bhargava, R. Ranchal, N. Singh, L. Lilien, L.B. Othmane 29th IEEE Symposium on Reliable Distributed System (SRDS) 2010
- *Privacy in Cloud Computing Through Identity Management* - B. Bhargava, N. Singh, A. Sinclair, International Conference on Advances in Computing and Communication ICACC-11, April, 2011, India.

- Active Bundle
- Anonymous Identification
- Computing Predicates with encrypted data
- Multi-Party Computing
- Selective Disclosure

Proposed IDM: 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

Proposed IDM: Active Bundle (Cont.)

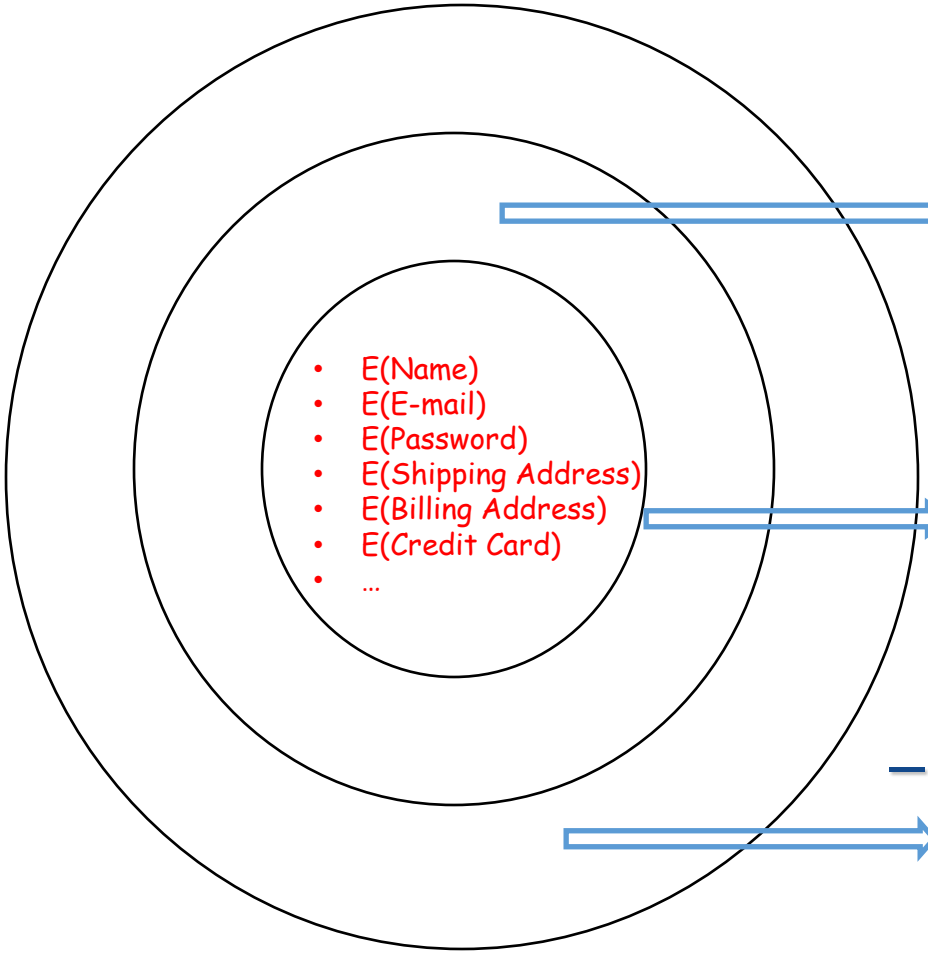
- Active Bundles—Operations
  - Self-Integrity check

    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

Proposed IDM: Active Bundle Scheme



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

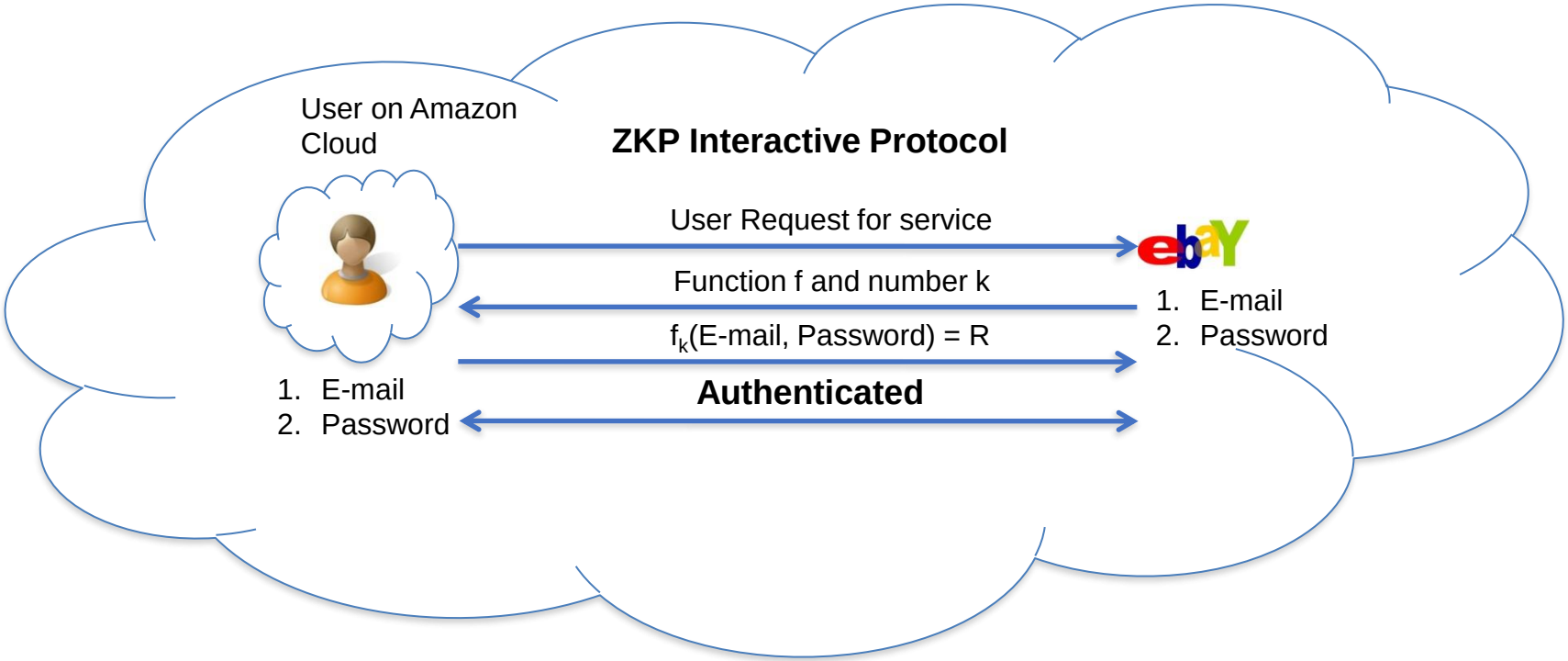
– **Sensitive Data:**
- Identity Information
- …

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

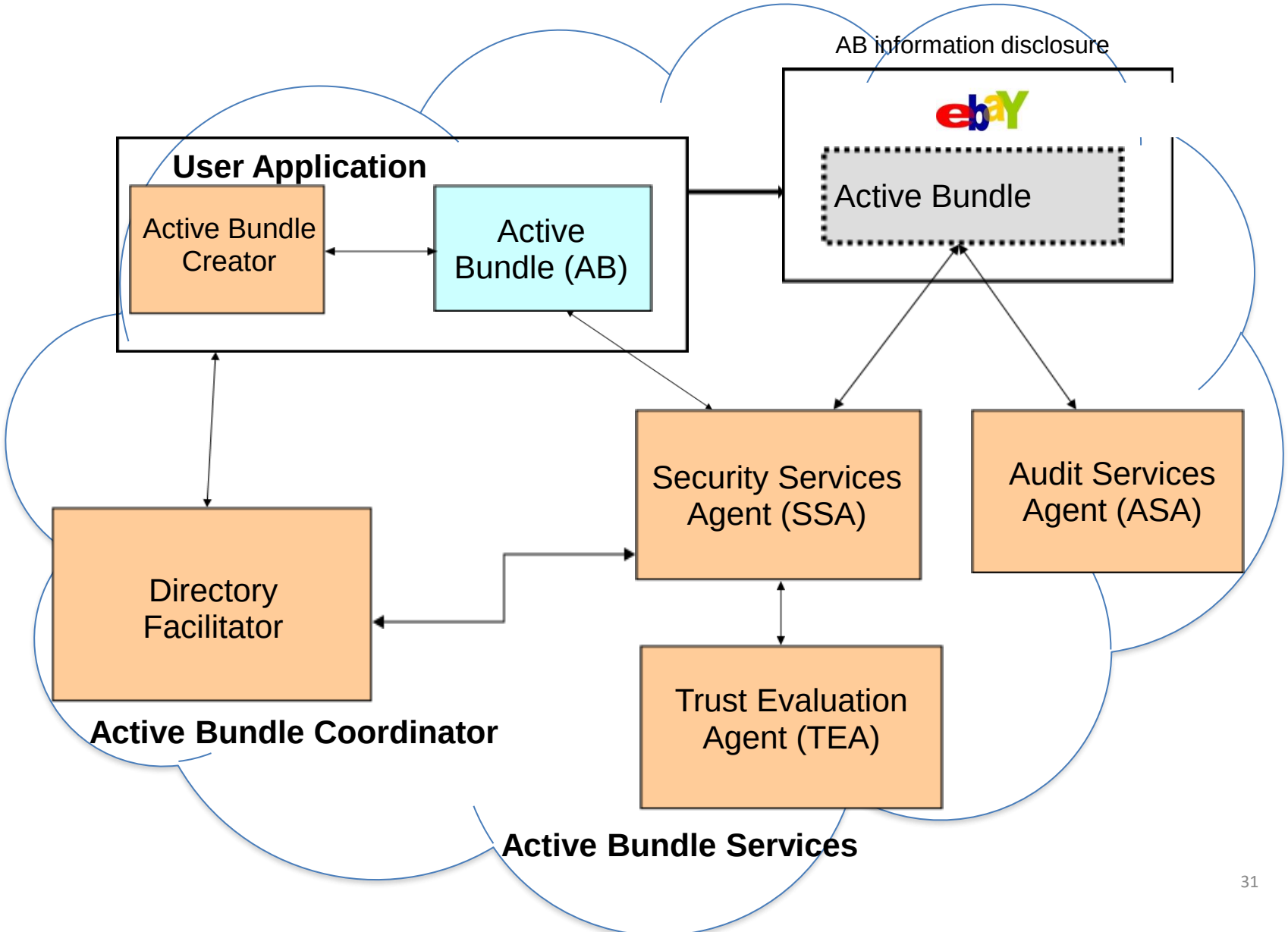
*** E( ) - Encrypted Information**

Proposed IDM: Anonymous Identification

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

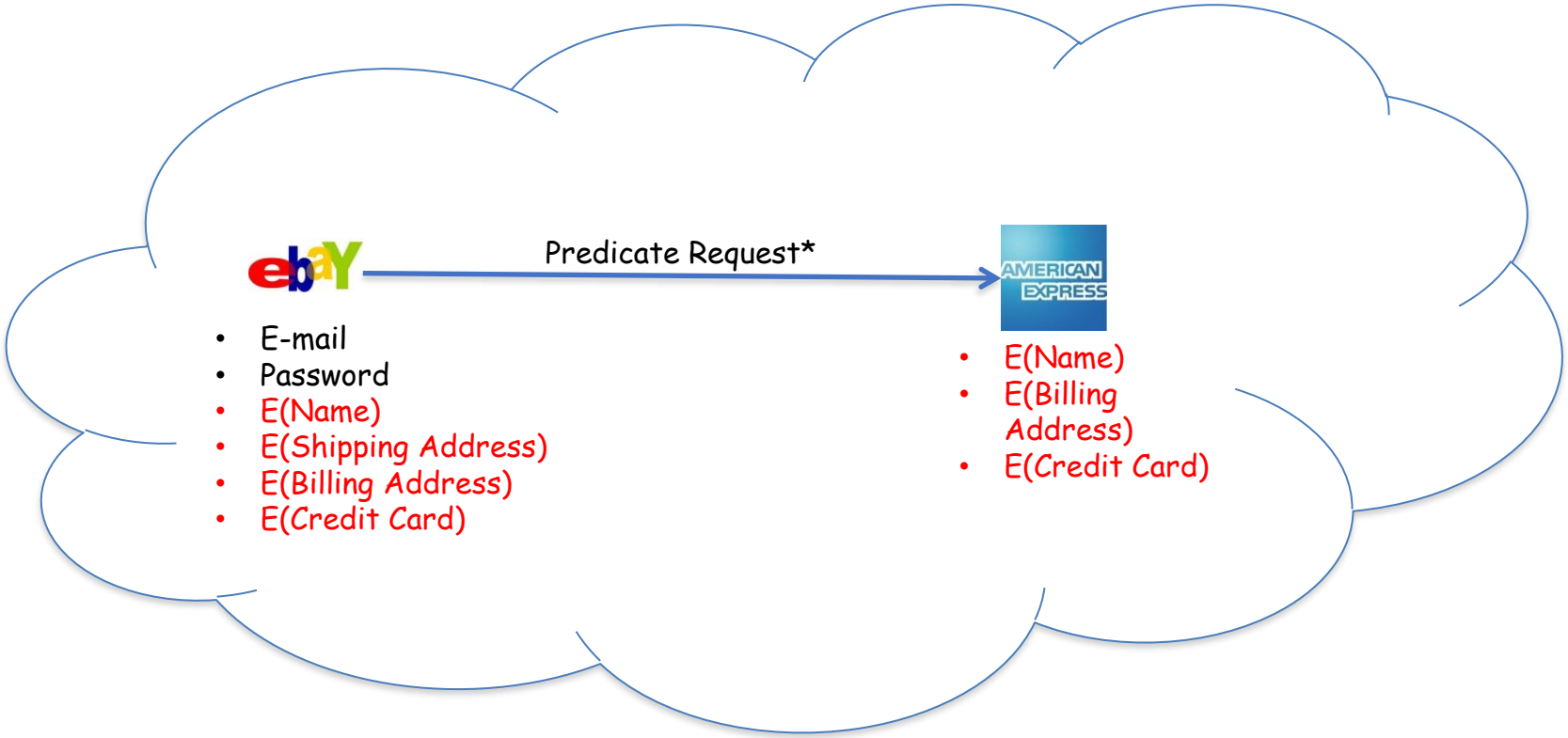


Proposed IDM:
Interaction using Active Bundle



Proposed IDM: Predicate over Encrypted Data

- Verification without disclosing unencrypted identity data.

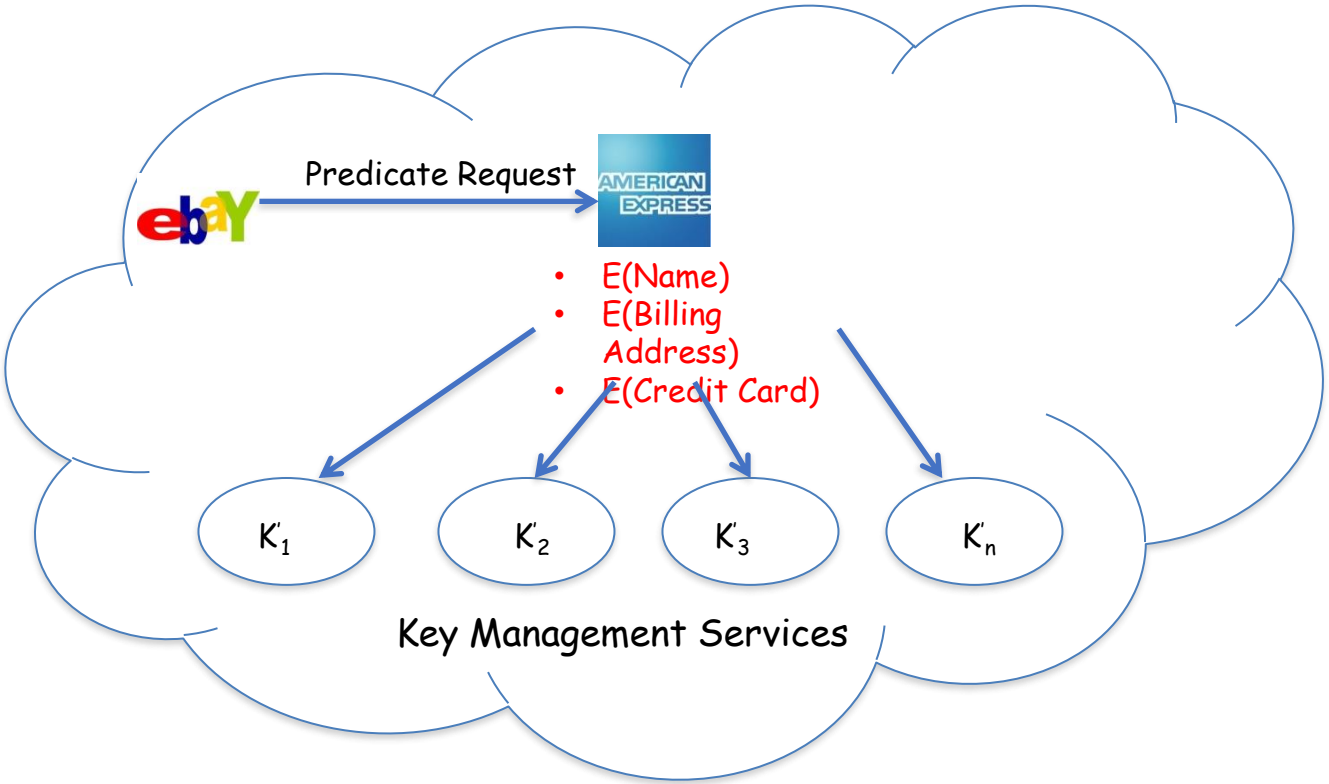


*Age Verification Request

*Credit Card Verification Request

Proposed IDM: Multi-Party Computing

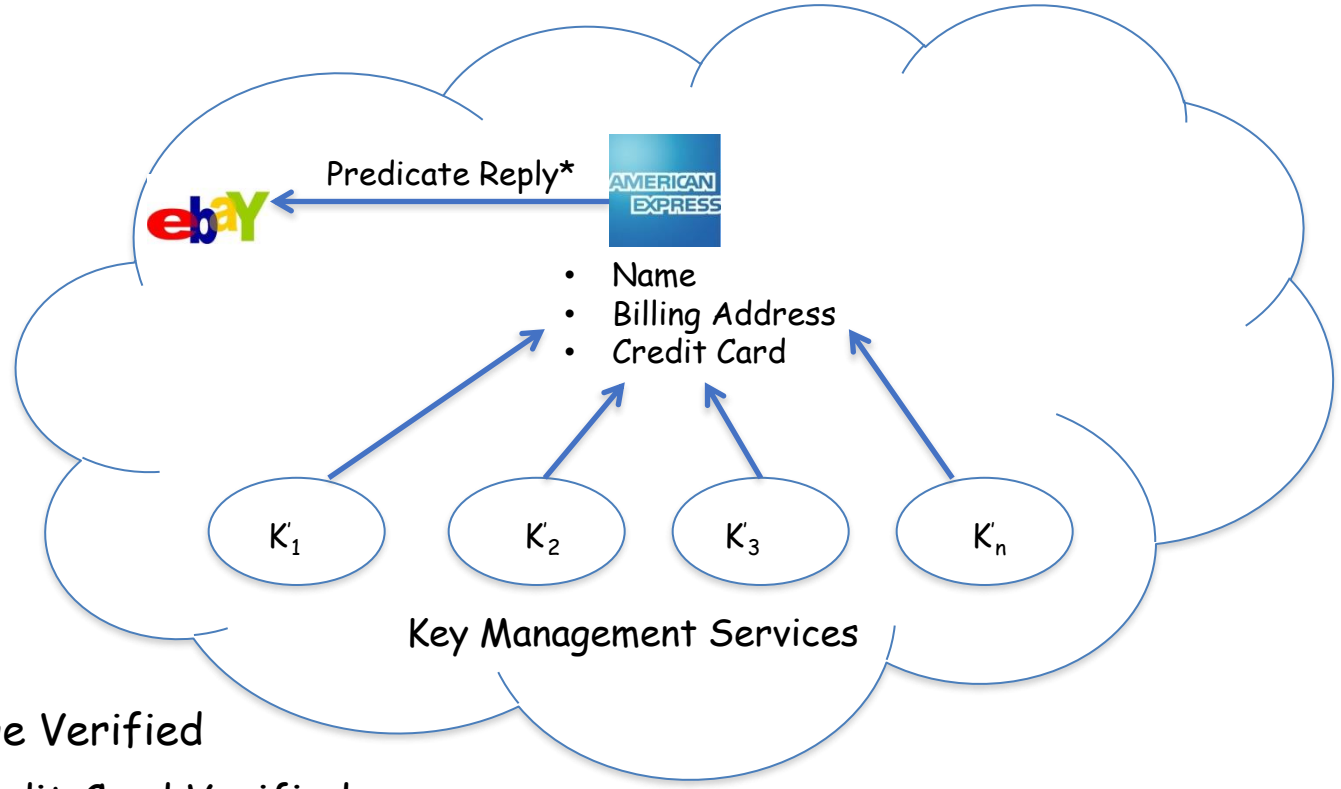
- To become independent of a trusted third party
  - Multiple Services hold shares of the secret key
  - Minimize the risk



* Decryption of information is handled by the Key Management services

Proposed IDM: Multi-Party Computing

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

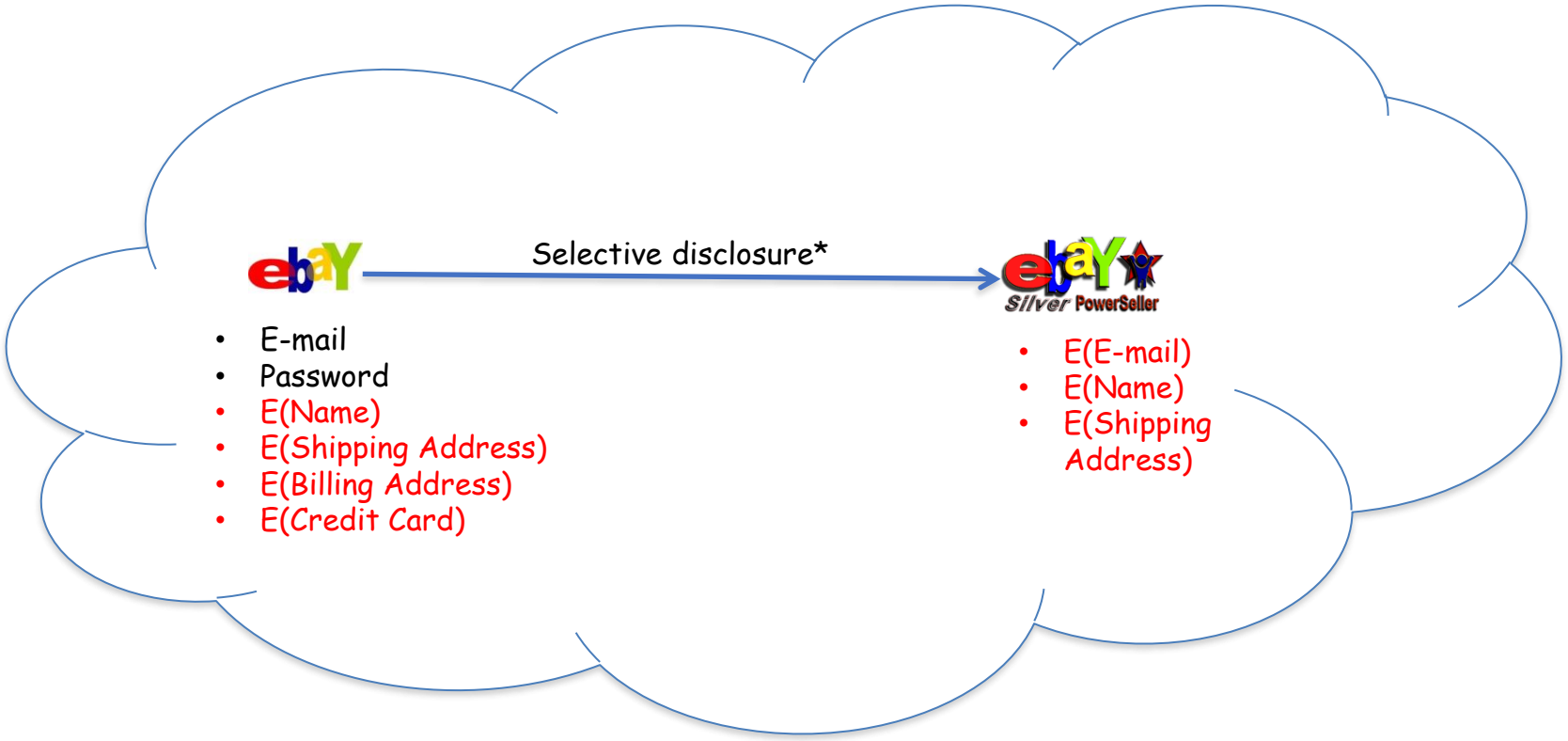


*Age Verified

*Credit Card Verified

Proposed IDM: Selective Disclosure

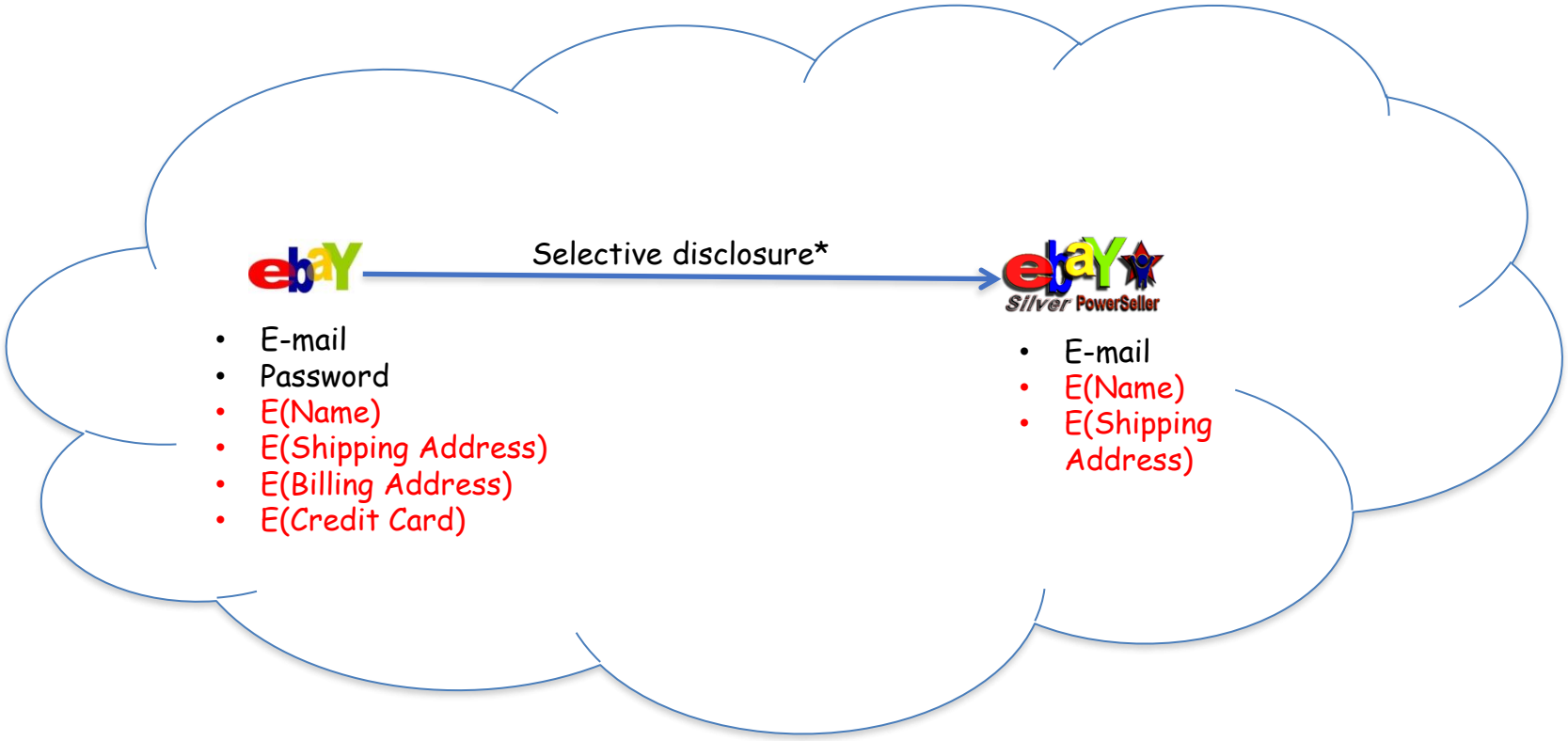
- User Policies in the Active Bundle dictate dissemination



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

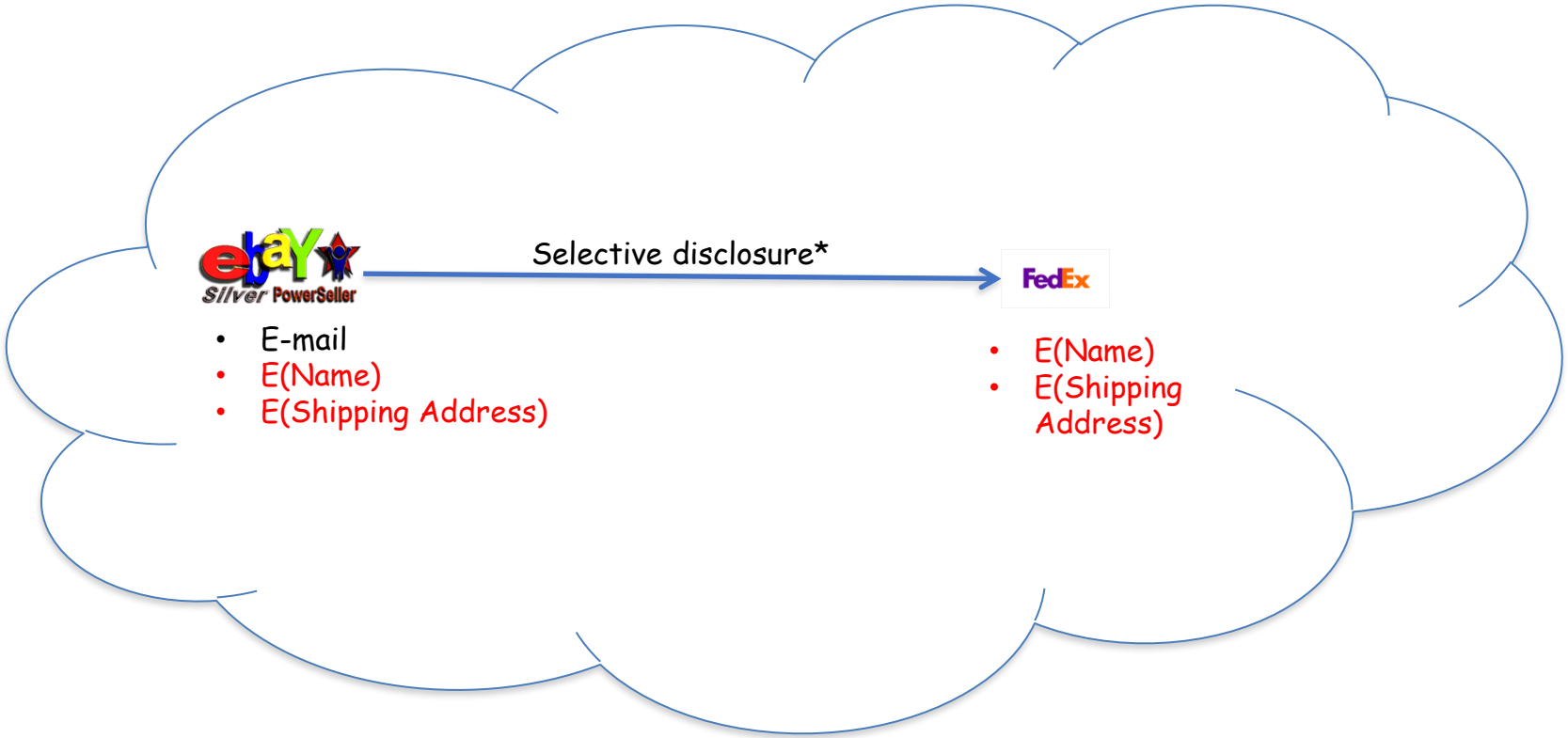
Proposed IDM: Selective Disclosure

- User Policies in the Active Bundle dictate dissemination



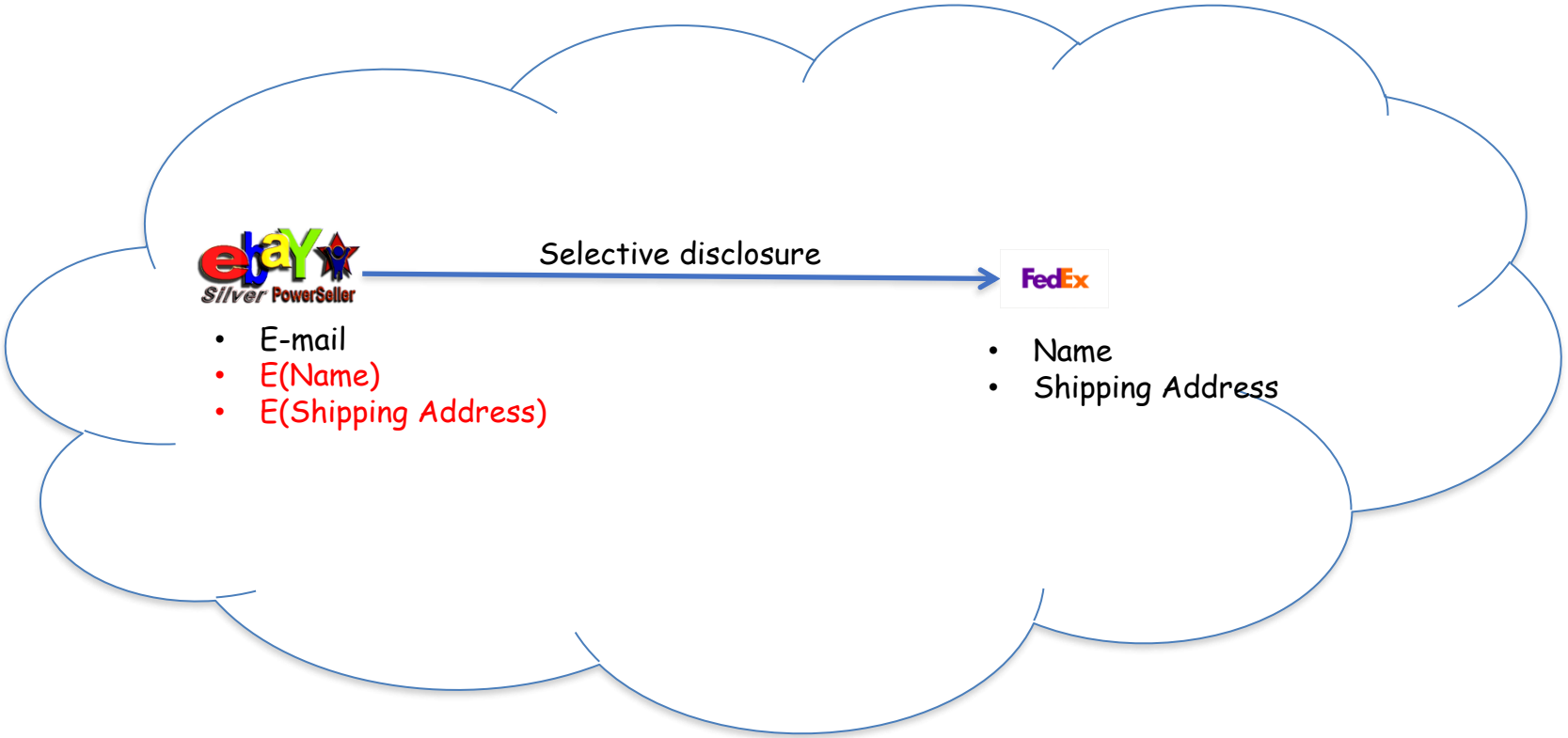
Decryption handled by Multi-Party Computing as in the previous slides

Proposed IDM: Selective Disclosure



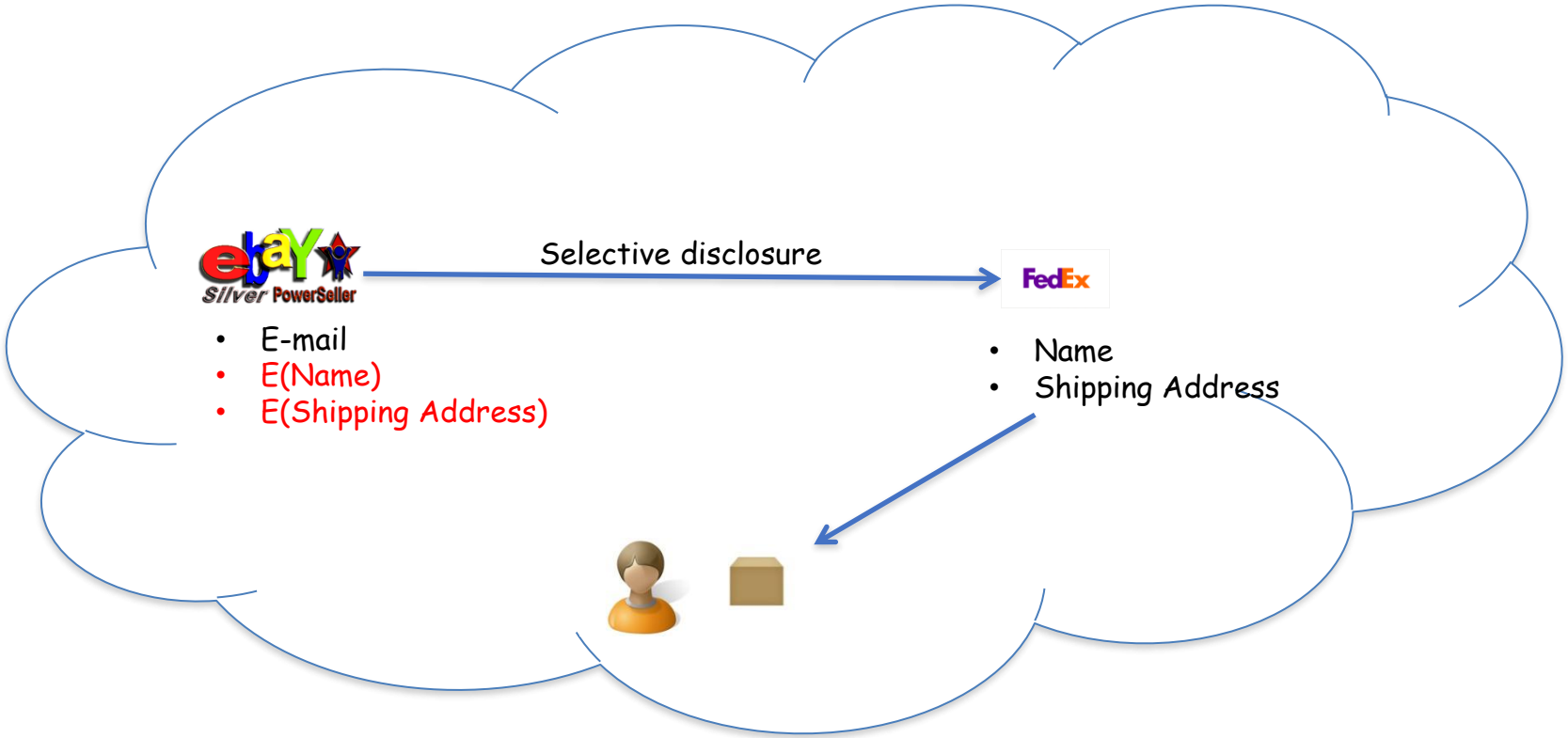
*e-bay seller shares the encrypted information based on the user policy

Proposed IDM: Selective Disclosure



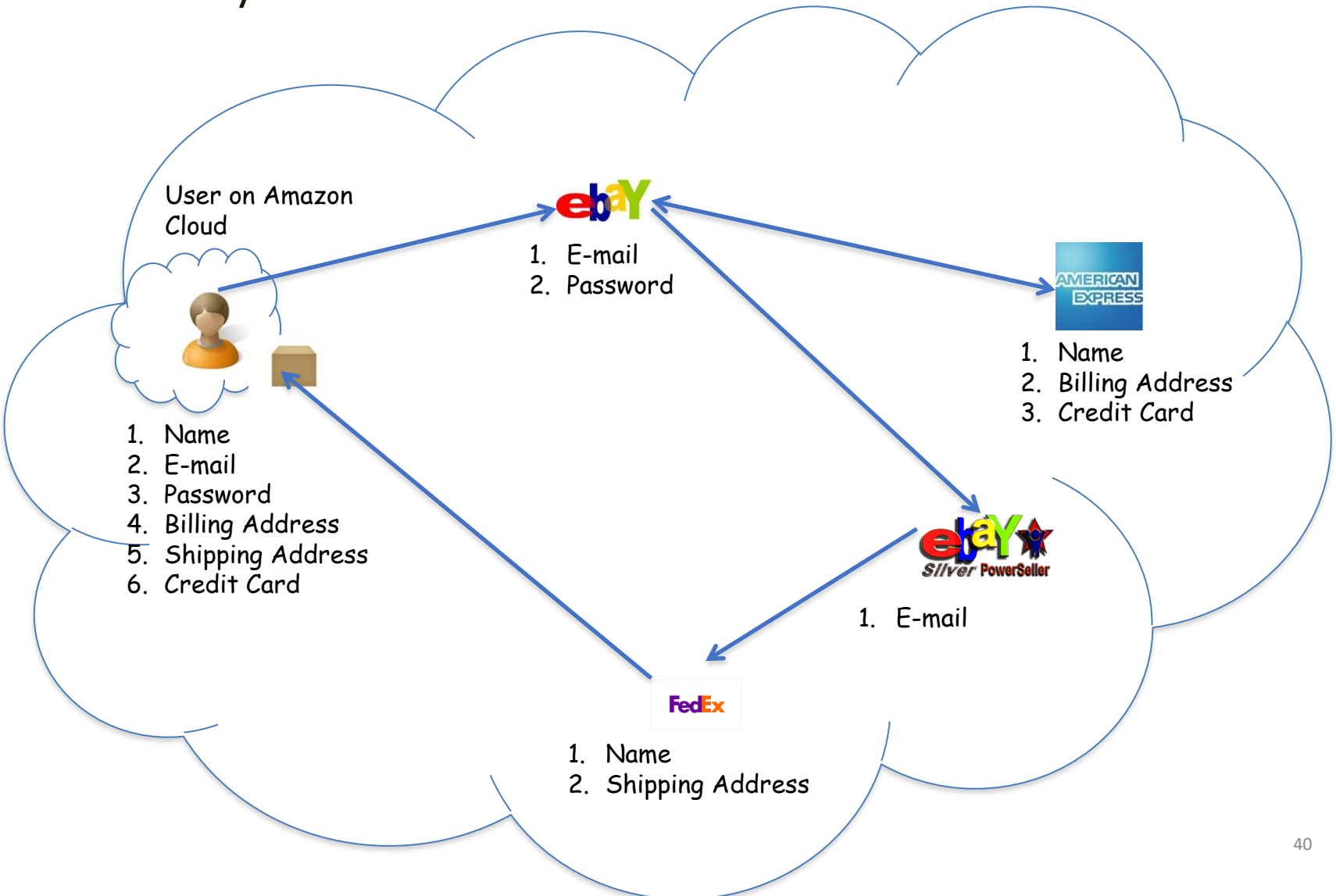
- Decryption handled by Multi-Party Computing as in the previous slides

Proposed IDM: Selective Disclosure



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

Proposed IDM: Identity in the Cloud



Proposed IDM: 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
- Independent of Third Party
  - Prevents correlation attacks
- Establishes the trust of users in IDM
  - Through putting the user in control of who has his data
  - Identity is being used in the process of authentication, negotiation, and data exchange.
- Minimal disclosure to the SP
  - SP receives only necessary information.

Proposed IDM: 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
- Future work
  - Develop the prototype, conduct experiments and evaluate the approach

Minimize Multi-tenancy

Minimize Multi-tenancy

- Can’t really force the provider to accept less tenants
  - Can try to increase isolation between tenants
    - Strong isolation techniques (VPC to some degree)
      - C.f. VM Side channel attacks (T. Ristenpart et al.)
    - QoS requirements need to be met
    - Policy specification
  - Can try to increase trust in the tenants
    - Who’s the insider, where’s the security boundary? Who can I trust?
    - Use SLAs to enforce trusted behavior

Conclusion

- Cloud computing is sometimes viewed as a reincarnation of the classic mainframe client-server model
  - However, resources are ubiquitous, scalable, highly virtualized
  - Contains all the traditional threats, as well as new ones
- In developing solutions to cloud computing security issues it may be helpful to identify the problems and approaches in terms of
  - Loss of control
  - Lack of trust
  - Multi-tenancy problems