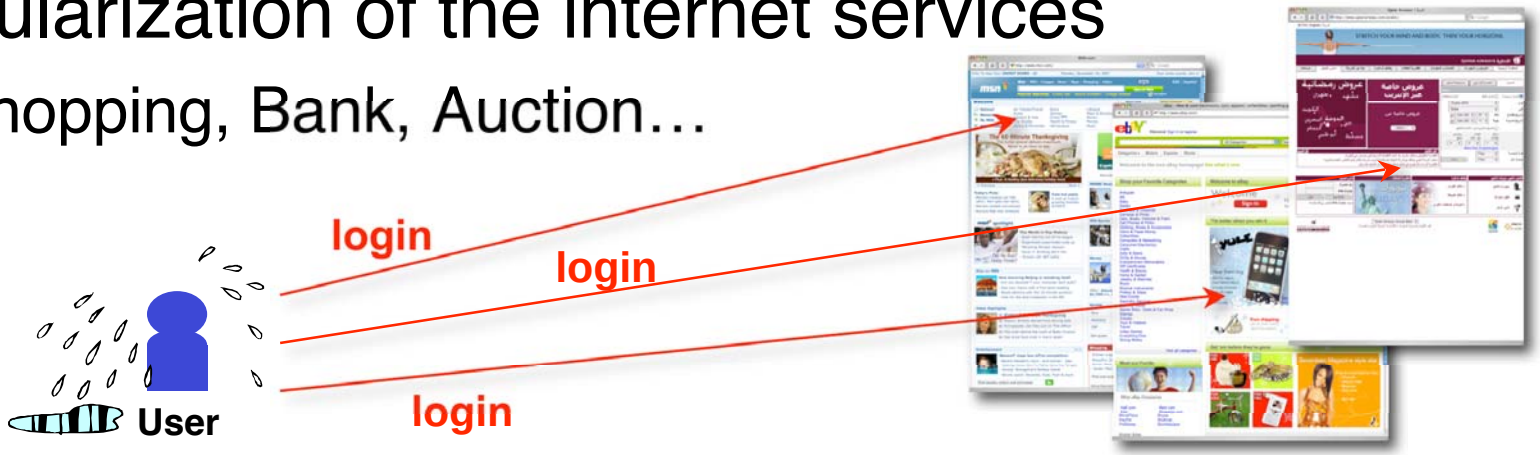
Privacy Enhancing Credential

National Institute of
Information and Communications Technology
(Japan)

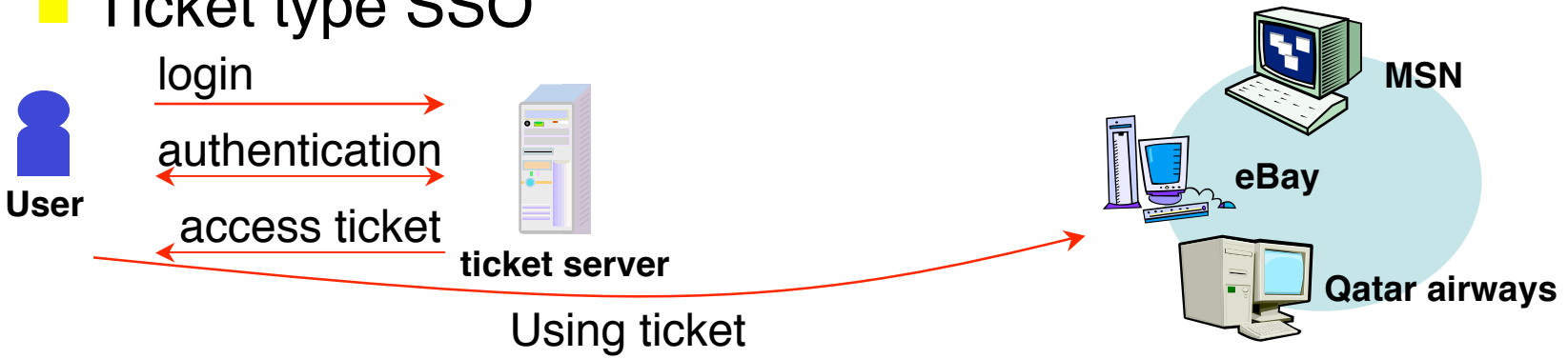
○ Junji Nakazato
Lihua Wang
Akihiro Yamamura

Motivation

- Popularization of the internet services
  - Shopping, Bank, Auction…

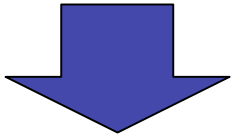


- Using single sign on (SSO) technique
  - Ticket type SSO



Motivation

- Disadvantages of SSO
  - The same ticket is used for multiple services
  - The user's privacy is obtained by the collusion with services
    - Use frequency of service
    - An order of using service
  - The user can transfer ticket to another user



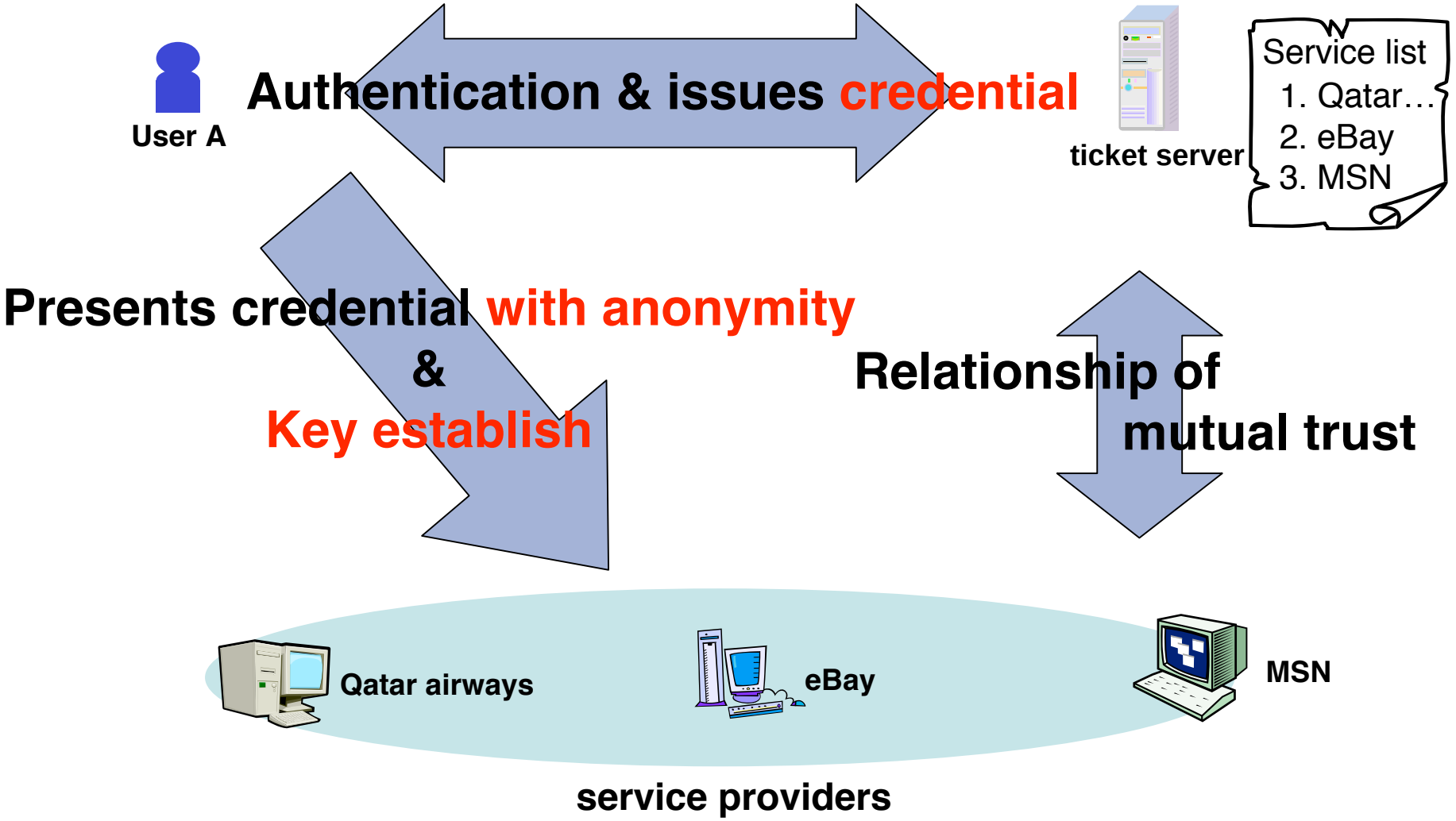
Needs to think about privacy!!

Our goal

- Multiple logins are not needed
  - The user only presents credential of whether he has the right to access service
- User's privacy is concealed
  - The user can access services with anonymity
- Credential cannot be transferred to anyone
  - No one can transfer correct credential to others
- Authenticated key exchange
  - To provide secure channel between user and service provider

Try to apply "credential system"

Our goal


User A
Authentication & issues credential
ticket server
Service list
1. Qatar…
2. eBay
3. MSN
Presents credential with anonymity
&
Key establish
Relationship of
mutual trust
Qatar airways
eBay
MSN
service providers

Credential system

- Previous work
  - "Designated Group Credentials"
  - Ching Yu Ng, Willy Susilo, Yi Mu
  - ASIACCS 2006

  - Using pairing technique
  - Authority can designate the verifiers
    - Ticket issuer can designate the service providers
  - The user authentication is necessary for the outside
  - The authority can trace user's movement
  - The user can transfer correct credential to others

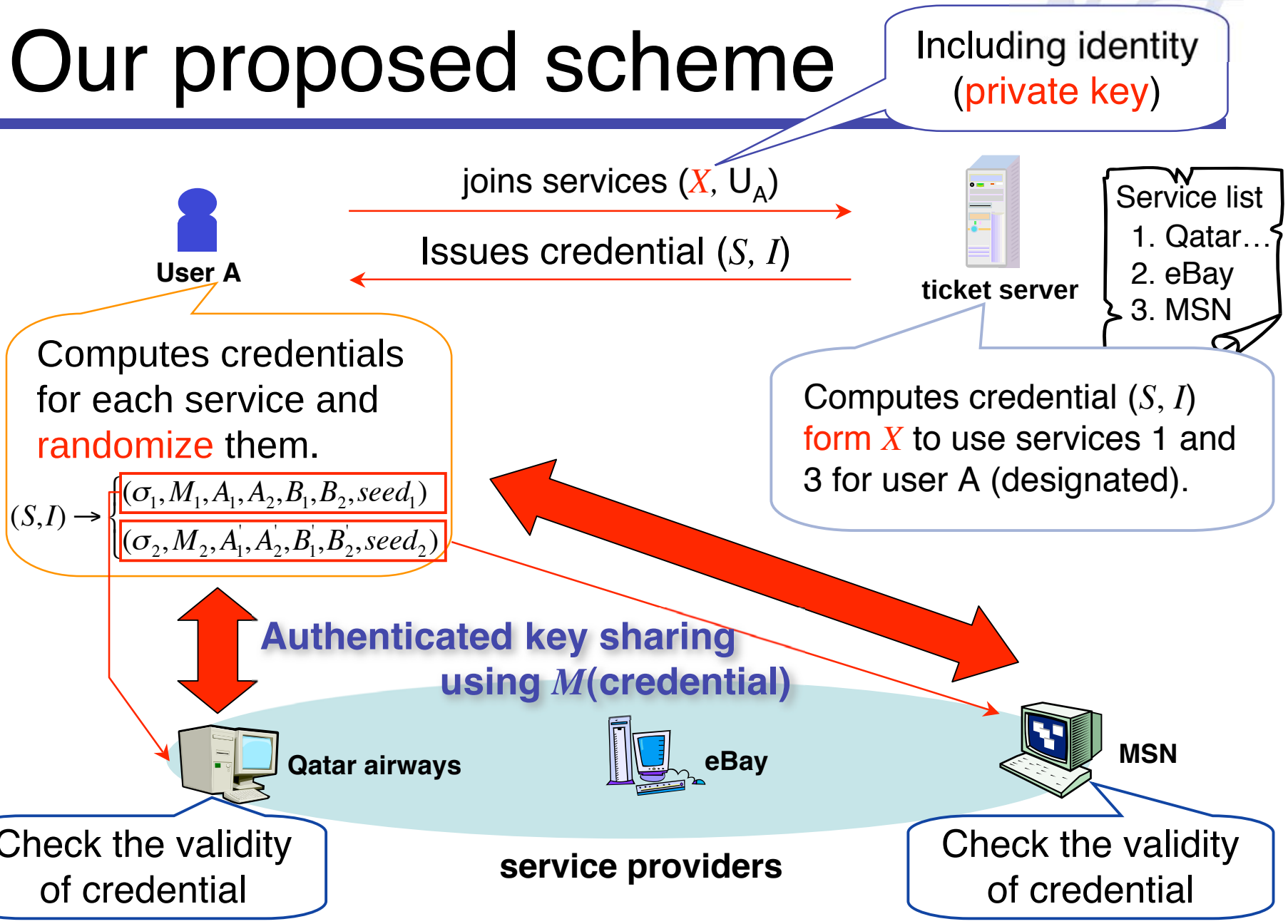
Comparison of requirements

	Group credential [4]	Our proposal
Unforgeability	Yes	Yes
Designated	Yes	Yes
Non-transferability	No	Yes
Anonymity	No	Yes
Unlinkability	No	Yes

Technique

- Based on pairing
  - Bilinear: Given any Q, R in $\boldsymbol{G}_1$ and a, b in $\boldsymbol{Z}_q$, we have $\mathrm{e}(aQ, bR) = \mathrm{e}(Q, R)^{ab}$
  - Non-degenerate: $\mathrm{e}(P, P) \neq 1$
  - Computable: There is an efficient algorithm to compute $\mathrm{e}(Q, R)$ for any Q, R in G_1
- Non-transferability
  - private key of user is included in the credential
- Unlinkability
  - Randomize credential when he uses it

Our proposed scheme



Conclusion

- Propose privacy enhancing credential
  - We preserved unlinkability (anonymity).
  - We satisfied non-transferability.
  - We achieved authenticated key exchange.

- We can provide time restriction function
  - It can be achieved by a few modification.
  - Change generator F to $\mathrm{h}(t)$
  - $\mathrm{h}()$: hash function $(\mathrm{h}(*) \rightarrow G_1)$

Thanks

独立行政法人
情報通信研究機構
National Institute of Information and Communications Technology