Anonymity 2.0: X.509 Extensions Supporting Privacy-Friendly Authentication

Vicente Benjumea[1], Seung Geol Choi[2], Javier Lopez[1] and Moti Yung[3]

[1] Computer Science Dpt. University of Malaga. Spain

[2] Computer Science Dpt. Columbia University. USA

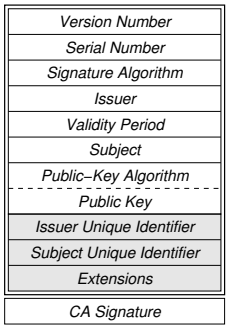
[3] Google Inc. & Computer Science Dpt. Columbia University. USA

Agenda

1. X.509 Certificates
2. Digital Signatures
3. Extending the Semantic of X.509 Certificates
4. The X.509 Public Key Certificate Extension
5. Incorporating New Signature Schemes into the X.509 Framework
6. Paradigm Integration
7. Conclusions

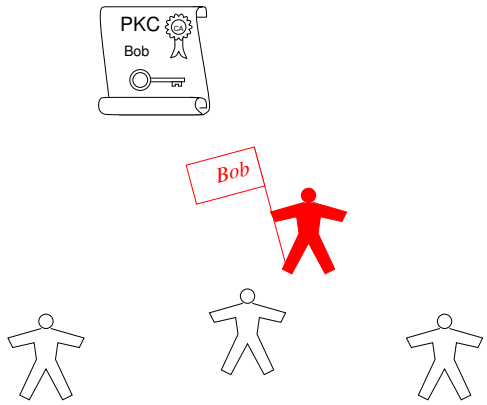
X.509 Certificates

- X.509 Public Key Certificates (PKC)
  - Bind a public key to a subject (person or entity)
  - The subject is the only one that knows the corresponding private key
  - Provide a suitable approach to **authentication**



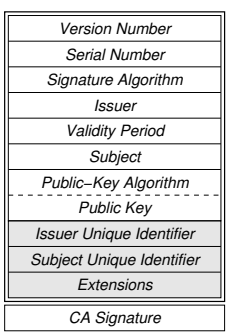
Public Key Certificate


Certification Authority



X.509 Certificates

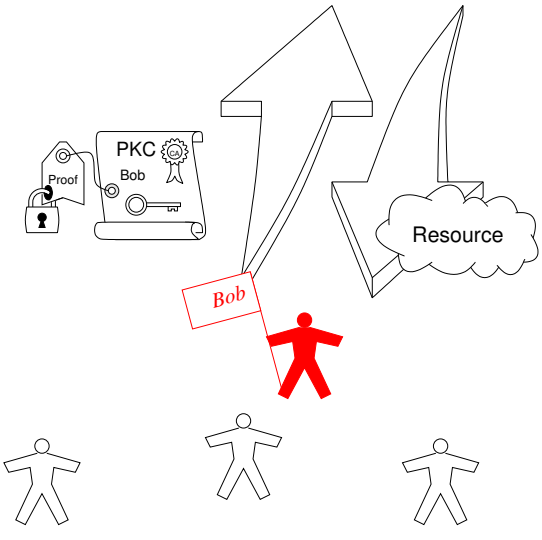
- X.509 Public Key Certificates (PKC)
  - Bind a public key to a subject (person or entity)
  - The subject is the only one that knows the corresponding private key
  - Provide a suitable approach to **authentication**



Public Key Certificate

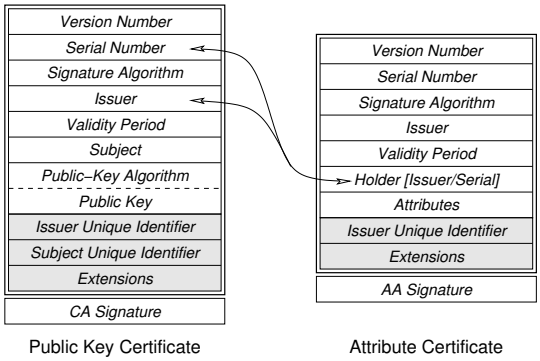

Certification Authority

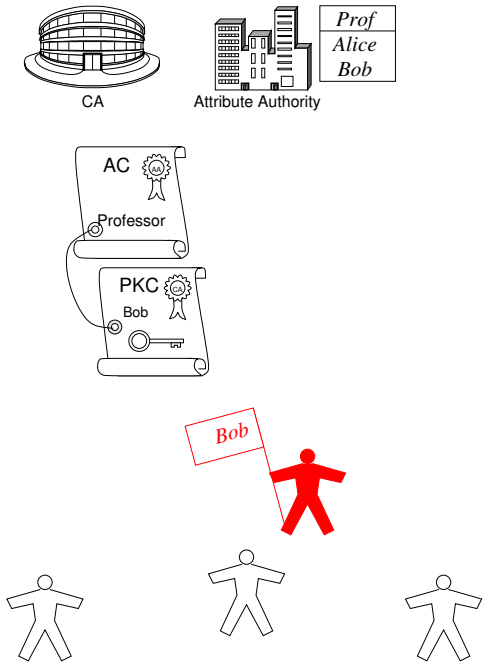
Service Provider



X.509 Certificates

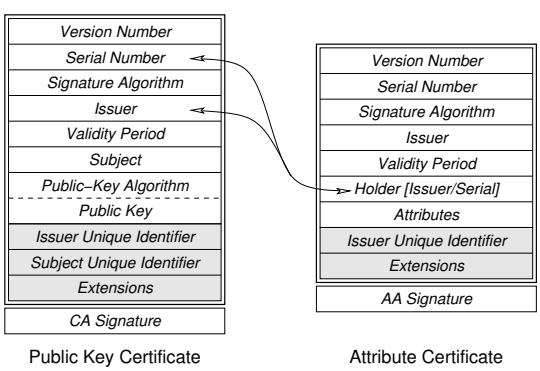
- X.509 Attribute Certificates (AC)
  - Bind attributes to a holder (usually a PKC)
  - The holder of the attribute is usually the subject of a linked PKC
  - Provide a suitable approach to **authorization**

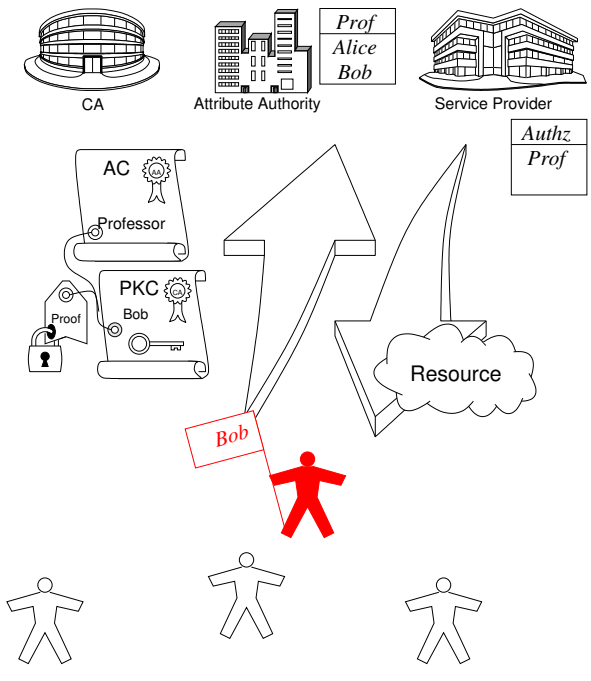




X.509 Certificates

- X.509 Attribute Certificates (AC)
  - Bind attributes to a holder (usually a PKC)
  - The holder of the attribute is usually the subject of a linked PKC
  - Provide a suitable approach to **authorization**





Privacy and Information Technologies

- Both approaches threaten the individual's **privacy**
  - All transactions carried out by individuals are **recorded**
  - The problem **increases** as long as the amount of transactions increases
  - All transactions in an individual's **whole life** can be recorded and cross-referenced

Agenda

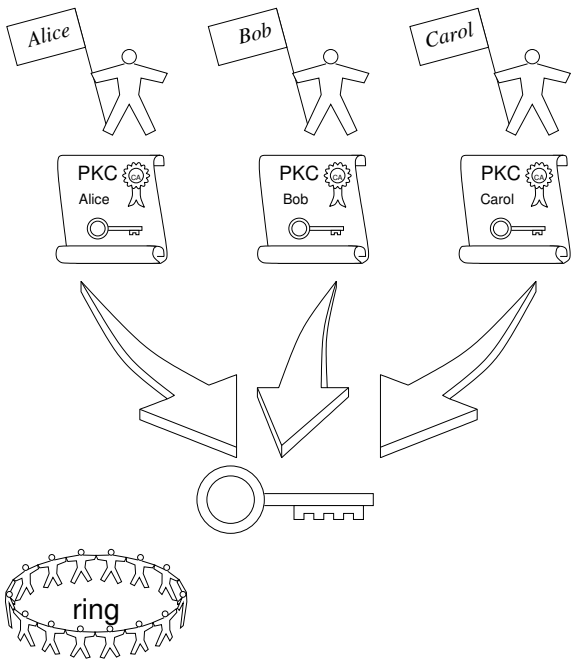
Digital Signatures for Anonymity

- Recently, new signature schemes have arisen focused on supporting anonymity
  - Ring signatures [Rivest et al:2001, Dodis et al:2004]
    - Irreversible anonymity
  - Group signatures [Chaum et al:1991, Ateniese et al:2000]
    - Reversible anonymity
  - Traceable signatures [Kiayias et al:2004]
    - Reversible & traceable anonymity

Digital Signatures for Anonymity

Ring Signatures (irreversible anonymity)

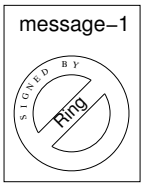
- RingSetup: creation of a ring of entities

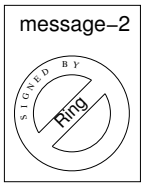


Digital Signatures for Anonymity

Ring Signatures (irreversible anonymity)

- RingSetup: creation of a ring of entities
- Sign: issue a ring signature (anon&unlink)

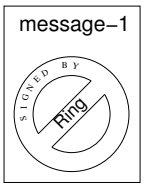


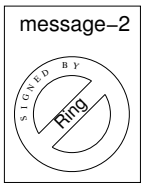


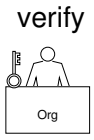
Digital Signatures for Anonymity

Ring Signatures (irreversible anonymity)

- RingSetup: creation of a ring of entities
- Sign: issue a ring signature (anon&unlink)
- Verify: verify a ring sign. (anon&unlink)







Digital Signatures for Anonymity

Ring Signatures (irreversible anonymity)

- RingSetup: creation of a ring of entities
- Sign: issue a ring signature (anon&unlink)
- Verify: verify a ring sign. (anon&unlink)

Group Signatures (reversible anonymity)

- GroupSetup: creation of a group

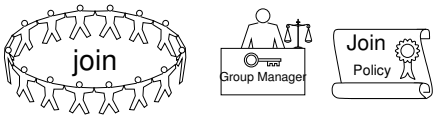
Digital Signatures for Anonymity

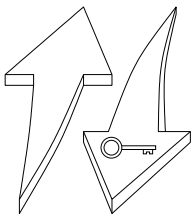
Ring Signatures (irreversible anonymity)

- RingSetup: creation of a ring of entities
- Sign: issue a ring signature (anon&unlink)
- Verify: verify a ring sign. (anon&unlink)

Group Signatures (reversible anonymity)

- GroupSetup: creation of a group
- Join: join to group





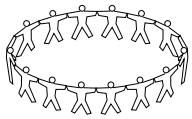
Digital Signatures for Anonymity

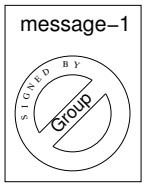
Ring Signatures (irreversible anonymity)

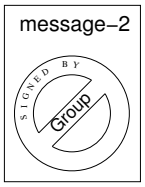
- RingSetup: creation of a ring of entities
- Sign: issue a ring signature (anon&unlink)
- Verify: verify a ring sign. (anon&unlink)

Group Signatures (reversible anonymity)

- GroupSetup: creation of a group
- Join: join to group
- Sign: issue a group sign. (anon&unlink)







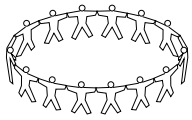
Digital Signatures for Anonymity

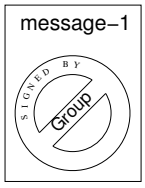
Ring Signatures (irreversible anonymity)

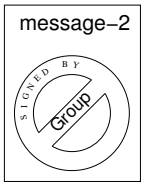
- RingSetup: creation of a ring of entities
- Sign: issue a ring signature (anon&unlink)
- Verify: verify a ring sign. (anon&unlink)

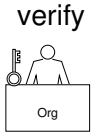
Group Signatures (reversible anonymity)

- GroupSetup: creation of a group
- Join: join to group
- Sign: issue a group sign. (anon&unlink)
- Verify: verify a group sign. (anon&unlink)









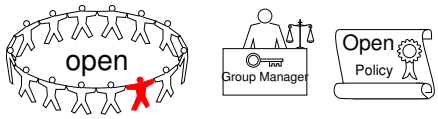
Digital Signatures for Anonymity

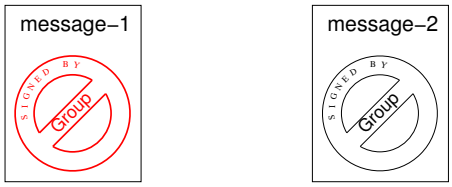
Ring Signatures (irreversible anonymity)

- RingSetup: creation of a ring of entities
- Sign: issue a ring signature (anon&unlink)
- Verify: verify a ring sign. (anon&unlink)

Group Signatures (reversible anonymity)

- GroupSetup: creation of a group
- Join: join to group
- Sign: issue a group sign. (anon&unlink)
- Verify: verify a group sign. (anon&unlink)
- Open: identify the issuing member





Digital Signatures for Anonymity

Ring Signatures (irreversible anonymity)

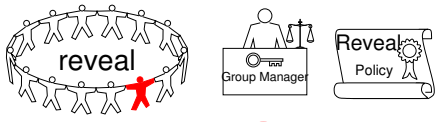
- RingSetup: creation of a ring of entities
- Sign: issue a ring signature (anon&unlink)
- Verify: verify a ring sign. (anon&unlink)

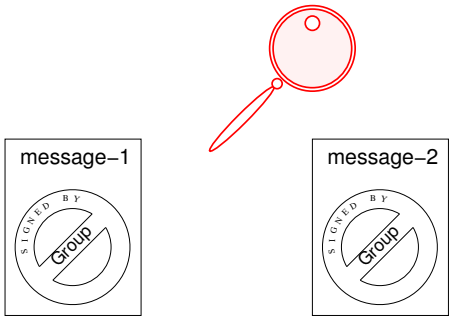
Group Signatures (reversible anonymity)

- GroupSetup: creation of a group
- Join: join to group
- Sign: issue a group sign. (anon&unlink)
- Verify: verify a group sign. (anon&unlink)
- Open: identify the issuing member

Traceable Signatures (GS +) (r&t anon.)

- Reveal: reveal member tracing trapdoor





Digital Signatures for Anonymity

Ring Signatures (irreversible anonymity)

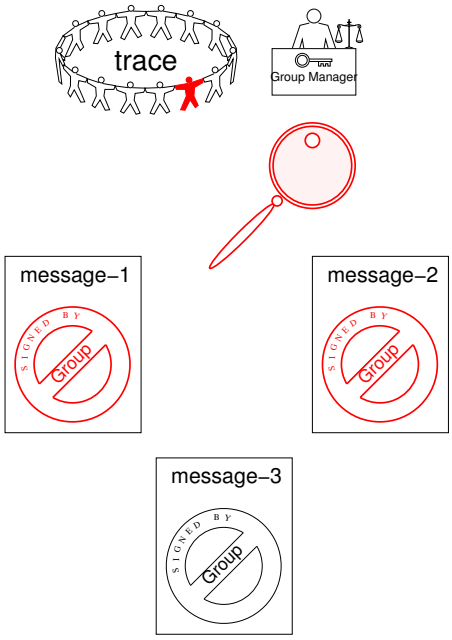
- RingSetup: creation of a ring of entities
- Sign: issue a ring signature (anon&unlink)
- Verify: verify a ring sign. (anon&unlink)

Group Signatures (reversible anonymity)

- GroupSetup: creation of a group
- Join: join to group
- Sign: issue a group sign. (anon&unlink)
- Verify: verify a group sign. (anon&unlink)
- Open: identify the issuing member

Traceable Signatures (GS +) (r&t anon.)

- Reveal: reveal member tracing trapdoor
- Trace: identify the signatures



Digital Signatures for Anonymity

Ring Signatures (irreversible anonymity)

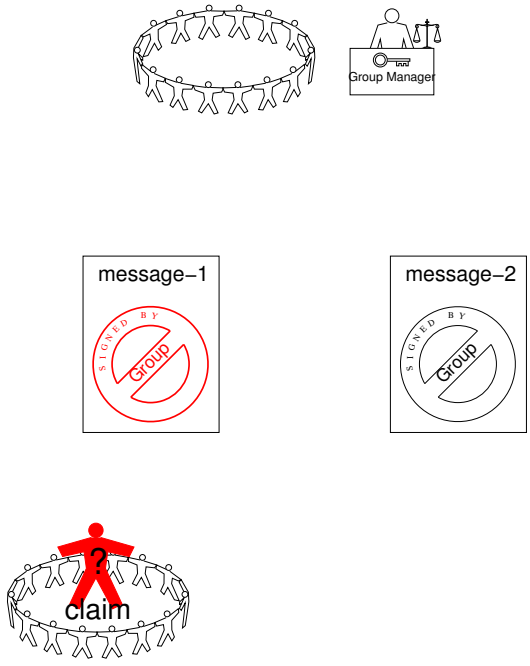
- RingSetup: creation of a ring of entities
- Sign: issue a ring signature (anon&unlink)
- Verify: verify a ring sign. (anon&unlink)

Group Signatures (reversible anonymity)

- GroupSetup: creation of a group
- Join: join to group
- Sign: issue a group sign. (anon&unlink)
- Verify: verify a group sign. (anon&unlink)
- Open: identify the issuing member

Traceable Signatures (GS +) (r&t anon.)

- Reveal: reveal member tracing trapdoor
- Trace: identify the signatures
- Claim: claim authorship



Agenda

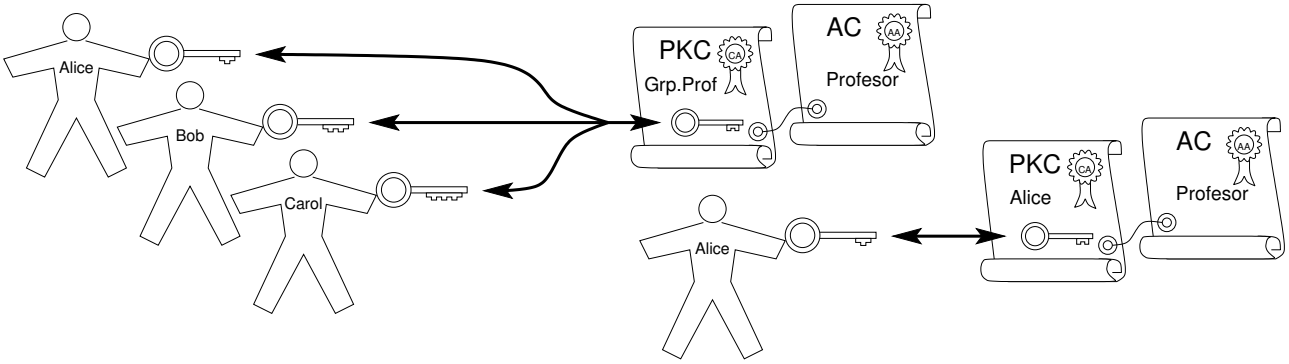
1. X.509 Certificates
2. Digital Signatures
3. Extending the Semantic of X.509 Certificates
4. The X.509 Public Key Certificate Extension
5. Incorporating New Signature Schemes into the X.509 Framework
6. Paradigm Integration
7. Conclusions

Semantic Extension to X.509 Certificates

- X.509 Certificates
  - Traditional (one-to-one) public key algorithms used in PKC are suited for scenarios based on identity authentication
  - However, many signature schemes (one-to-many) do not fit in this scenario (ring, group, traceable signatures and others)
- Proposal:
  - A semantic extension to X.509 certificates to allow the incorporation of these new signature schemes
  - Advantages for both worlds
    - The standard framework incorporates anonymity
    - Anonymous applications under a standard framework (interoperability, heterogeneity, infrastructure)

Semantic Extension to X.509 Certificates

- Proposal:
  - PKC binds a public key to a **concept** (concrete or abstract)
  - PKC binds the **concept** to the set of entities that own suitable private keys
  - The traditional semantic is also supported (included)
  - Traditional as well as new signature schemes are allowed
  - AC binds attributes to a PKC, as traditionally
  - But the attribute holder now relates to the PKC **concept**



Semantic Extension to X.509 Certificates

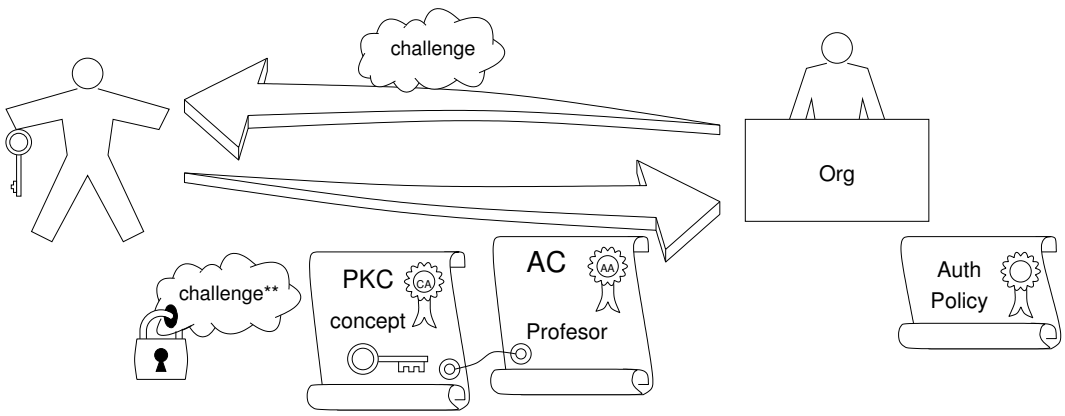
- Under the new semantic extension, entity authentication has a broader semantic
  - Identity authentication (traditional semantic)
    - When the PKC defines a concept that is the identity of a concrete single entity
  - Abstract authentication
    - When the PKC defines an abstract concept
  - Any entity (identified or anonymous), that owns a private key that can be verified with the public key in the PKC, can be authenticated as a proper holder of the PKC
  - A proper holder of a PKC is allowed to enjoy the privileges associated to the PKC itself and to the linked ACs
- The properties of the entity authentication depend on the properties of the used public key algorithm (signature scheme)

Agenda

1. X.509 Certificates
2. Digital Signatures
3. Extending the Semantic of X.509 Certificates
4. The X.509 Public Key Certificate Extension
5. Incorporating New Signature Schemes into the X.509 Framework
6. Paradigm Integration
7. Conclusions

The X.509 Public Key Certificate Extension

- The same structure holds. It entails the use of some already defined standard extension fields **plus** a new extension field: **certificateFeatures**
  - Provide useful usage information and state the PKC properties
- It can be used as usual (same protocols and structures), but with different properties (independent of the PK algorithm)
- The properties of the entity authentication depend on the properties of the used public key algorithm (signature scheme). Stated in the certificateFeatures field



Main Changes to the X.509 Public Key Certificate (standard extension fields)

- Public key algorithm: support for new signature schemes
  - ring, group, traceable, others
- Subject: support for concept description (distinguished name)
  - `GN=ProfessorGroup, CN=GroupManager, OU=CS, O=UMA, L=MA, ST=AND, C=ES`
  - `GN=ProfessorGroup, DNS=groupmanager@cs.uma.es`
- Key usage: digital-signature, non-repudiation
- Certificate policies: ring creation, join to group, membership resign, anonymity, etc
- CRL distribution points: certificate revocation list distribution points
- Authority information access:
  - OCSP certificate revocation status
  - OCSP+ member revocation status
  - Fairness authorities involved in safeguarding anonymity

Main Changes to the X.509 Public Key Certificate (**new extension field**)

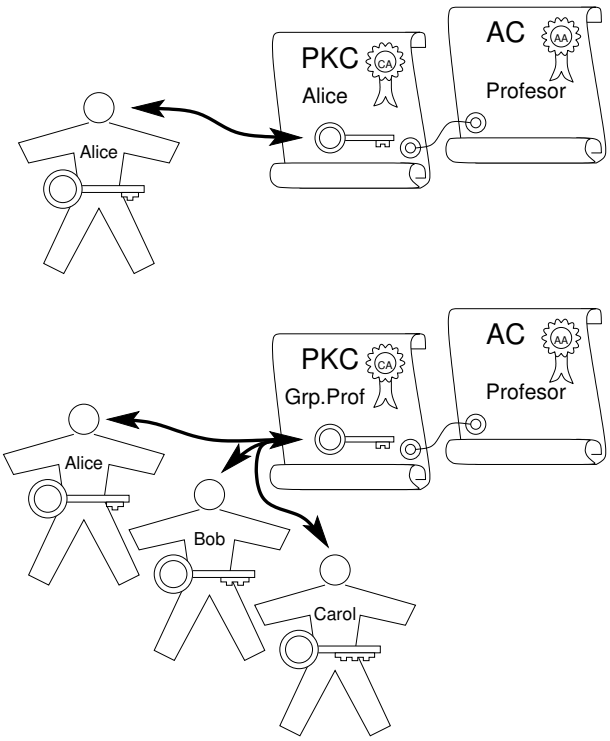
Certificate features: marked as **critical**

- Extended semantic

Main Changes to the X.509 Public Key Certificate (**new extension field**)

Certificate features: marked as **critical**

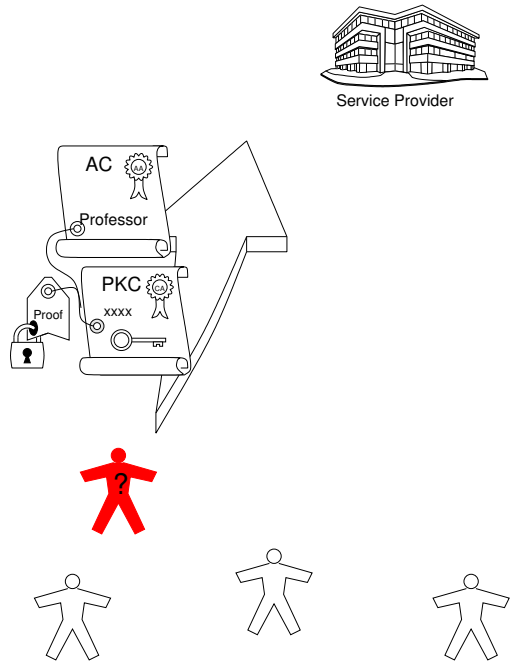
- Extended semantic
- One-to-many



Main Changes to the X.509 Public Key Certificate (**new extension field**)

Certificate features: marked as **critical**

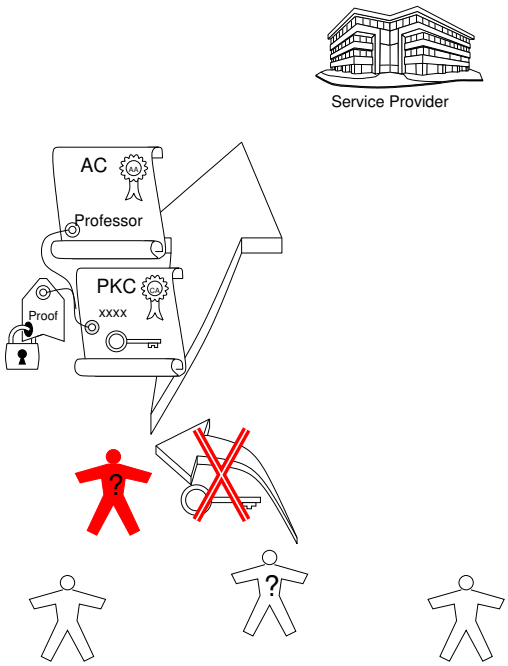
- Extended semantic
- One-to-many
- Anonymous



Main Changes to the X.509 Public Key Certificate (**new extension field**)

Certificate features: marked as **critical**

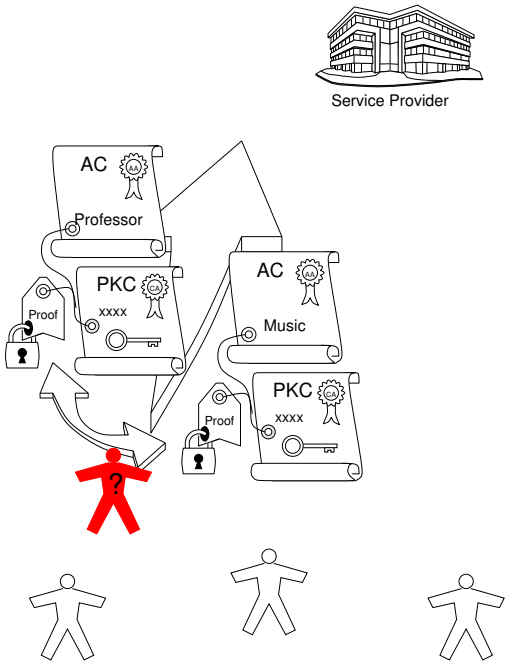
- Extended semantic
- One-to-many
- Anonymous
- Deter-sharing



Main Changes to the X.509 Public Key Certificate (**new extension field**)

Certificate features: marked as **critical**

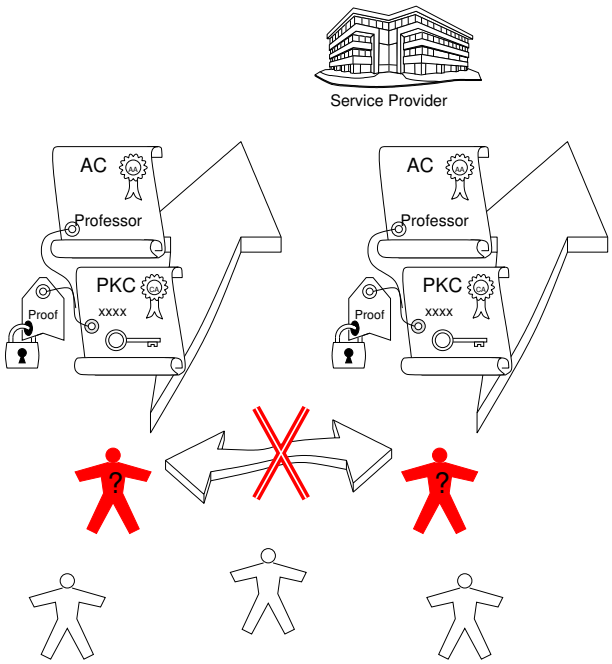
- Extended semantic
- One-to-many
- Anonymous
- Deter-sharing
- Multi-group



Main Changes to the X.509 Public Key Certificate (**new extension field**)

Certificate features: marked as **critical**

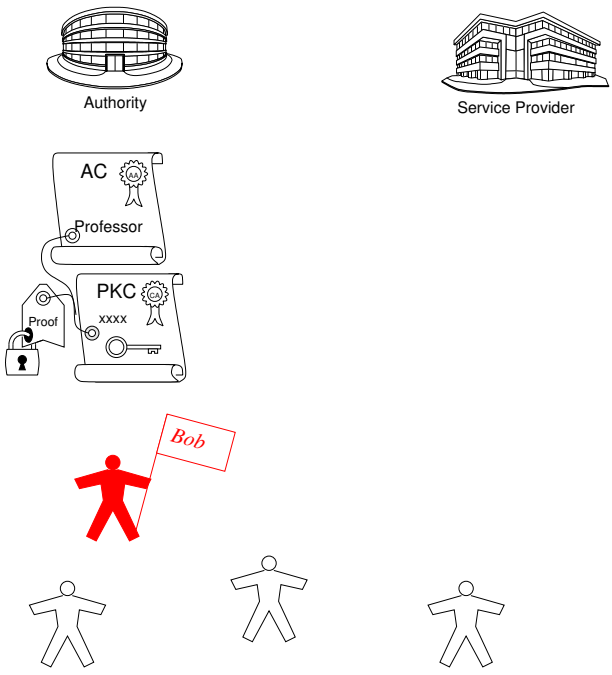
- Extended semantic
- One-to-many
- Anonymous
- Deter-sharing
- Multi-group
- Unlinkable



Main Changes to the X.509 Public Key Certificate (**new extension field**)

Certificate features: marked as **critical**

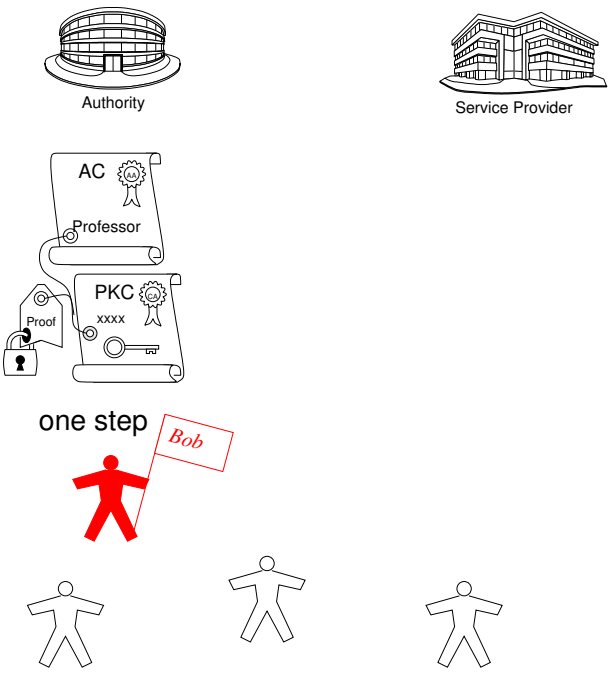
- Extended semantic
- One-to-many
- Anonymous
- Deter-sharing
- Multi-group
- Unlinkable
- Reversible



Main Changes to the X.509 Public Key Certificate (**new extension field**)

Certificate features: marked as **critical**

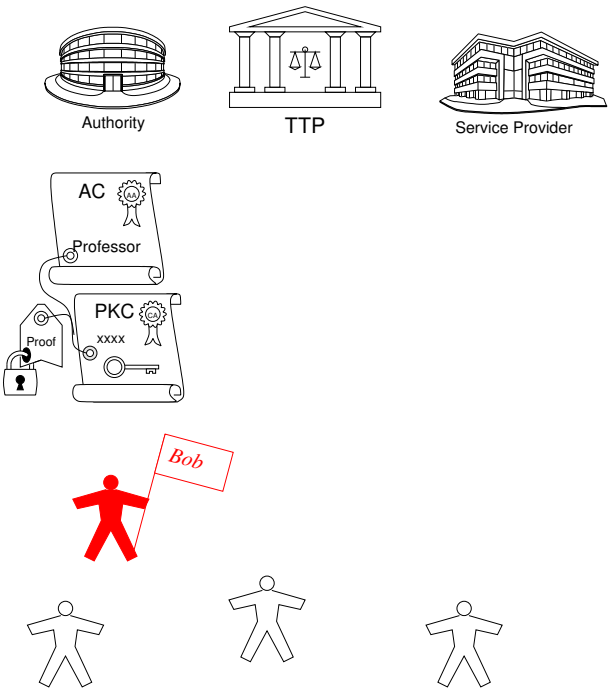
- Extended semantic
- One-to-many
- Anonymous
- Deter-sharing
- Multi-group
- Unlinkable
- Reversible
- One-level-anon



Main Changes to the X.509 Public Key Certificate (**new extension field**)

Certificate features: marked as **critical**

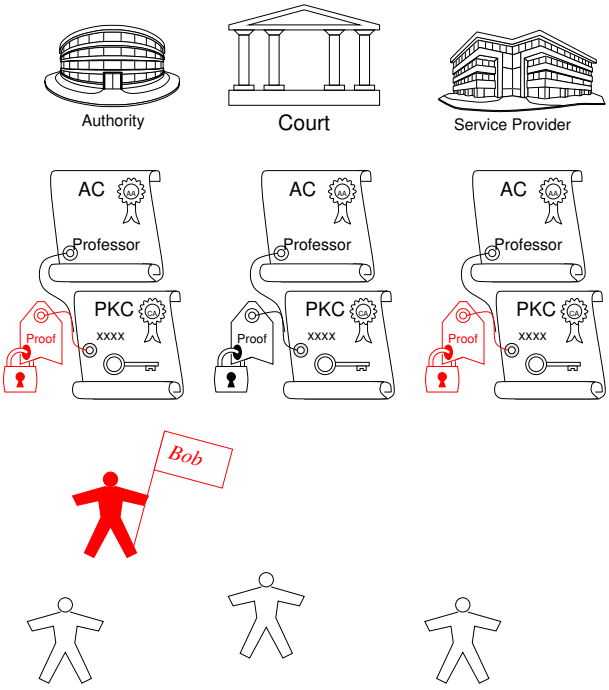
- Extended semantic
- One-to-many
- Anonymous
- Deter-sharing
- Multi-group
- Unlinkable
- Reversible
- One-level-anon
- Fairness



Main Changes to the X.509 Public Key Certificate (**new extension field**)

Certificate features: marked as **critical**

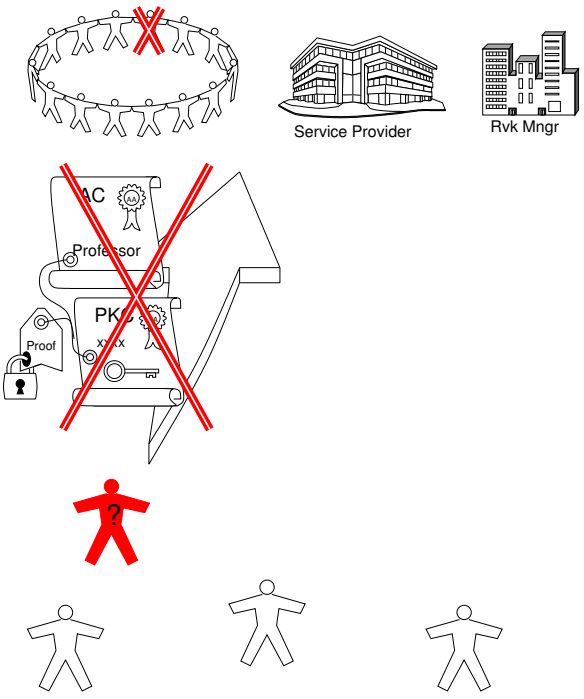
- Extended semantic
- One-to-many
- Anonymous
- Deter-sharing
- Multi-group
- Unlinkable
- Reversible
- One-level-anon
- Fairness
- Traceable



Main Changes to the X.509 Public Key Certificate (**new extension field**)

Certificate features: marked as **critical**

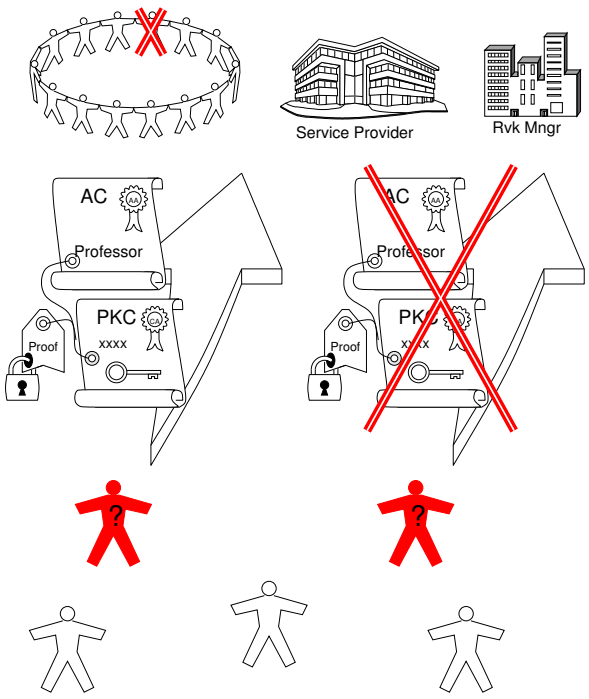
- Extended semantic
- One-to-many
- Anonymous
- Deter-sharing
- Multi-group
- Unlinkable
- Reversible
- One-level-anon
- Fairness
- Traceable
- Member-revocable



Main Changes to the X.509 Public Key Certificate (**new extension field**)

Certificate features: marked as **critical**

- Extended semantic
- One-to-many
- Anonymous
- Deter-sharing
- Multi-group
- Unlinkable
- Reversible
- One-level-anon
- Fairness
- Traceable
- Member-revocable
- Auth-revocable



Agenda

1. X.509 Certificates
2. Digital Signatures
3. Extending the Semantic of X.509 Certificates
4. The X.509 Public Key Certificate Extension
5. Incorporating New Signature Schemes into the X.509 Framework
6. Paradigm Integration
7. Conclusions

Incorporating Ring Signatures

- A privileged entity creates a ring with the public keys of its members, and requests the Certification Authority to issue a PKC binding the ring concept with the ring public key
- Any member of the ring can be anonymously authenticated with the PKC public key
- The authentication is anonymous, unlinkable and irreversible
- The PKC and the whole ring can be revoked

Incorporating Group Signatures

- A privileged entity creates a group, and requests the Certification Authority to issue a PKC binding the group concept with the group public key
- Users join the group if they are allowed to do so, based on some policy
- Any member of the group can be anonymously authenticated with the PKC public key
- The authentication is anonymous, unlinkable and reversible
- The group manager is able to correlate a given authentication with the corresponding member of the group
- The PKC and the whole group can be revoked

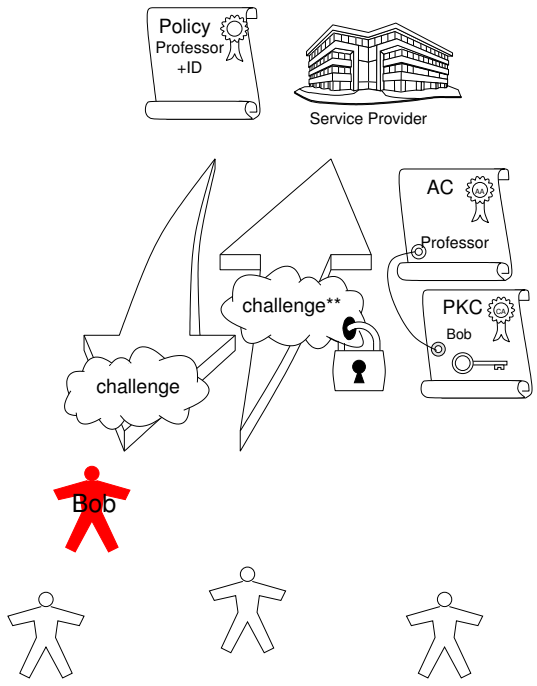
Incorporating Traceable Signatures

- The authentication is anonymous, unlinkable, reversible and traceable
- The group manager is also able to disclose a member tracing key that allows the tracing agents to trace authentications
- Also the member tracing key can be used to revoke members from the group

Agenda

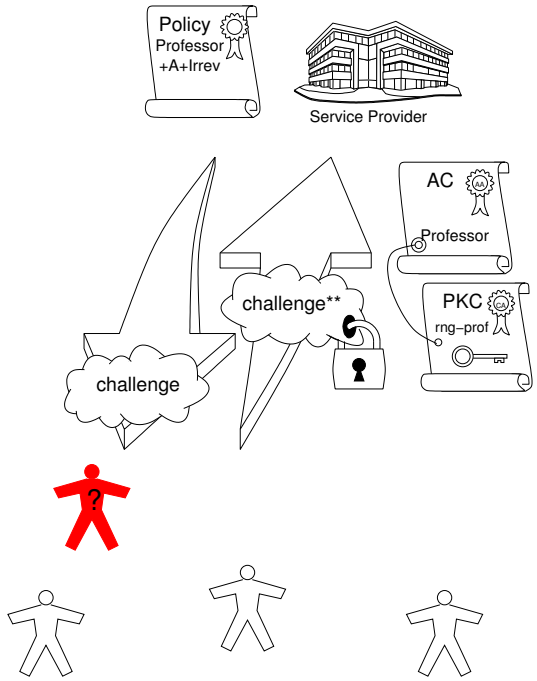
Paradigm Integration

- **Transparently** integrates anonymity
- Same authentication protocol
- Driven by the policy (privileges&mode)
  - Identity authentication



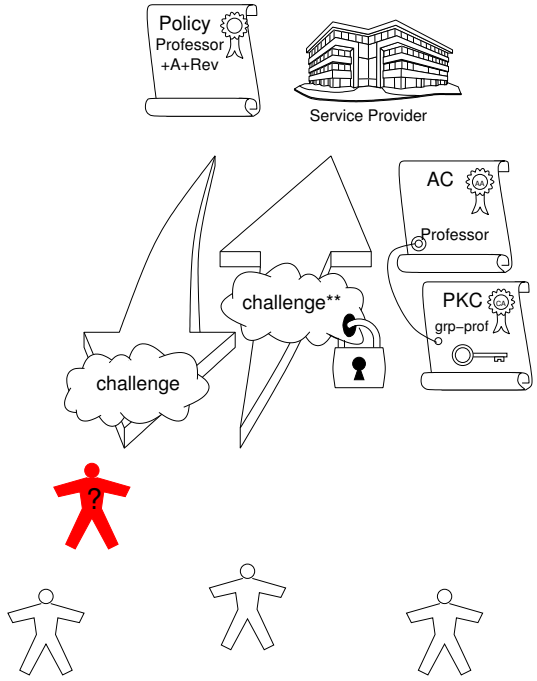
Paradigm Integration

- **Transparently** integrates anonymity
- Same authentication protocol
- Driven by the policy (privileges&mode)
  - Identity authentication
  - Anonymous auth. (irrev) [ring]



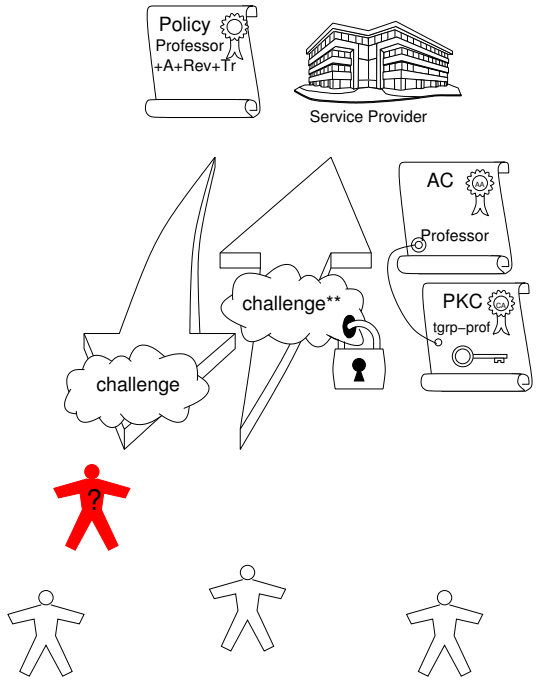
Paradigm Integration

- **Transparently** integrates anonymity
- Same authentication protocol
- Driven by the policy (privileges&mode)
  - Identity authentication
  - Anonymous auth. (irrev) [ring]
  - Anonymous auth. (rev) [group]



Paradigm Integration

- **Transparently** integrates anonymity
- Same authentication protocol
- Driven by the policy (privileges&mode)
  - Identity authentication
  - Anonymous auth. (irrev) [ring]
  - Anonymous auth. (rev) [group]
  - Anonymous auth. (rev&trac) [trac]
  - Others ...



Agenda

Conclusions

- A semantic extension has been proposed to incorporate new signature schemes into the X.509 standard framework
- Incorporates ring, group, traceable signatures and others
- It can also be applied to other standards (SPKI)
- It transparently supports identity and anonymous authentication
- Driven by the policy (privileges&mode)
- It is part of a system that integrates anonymous credentials into the X.509 framework based on the "fair traceable multi-group signature" scheme
- It fits into the Identity 2.0 effort (plus anonymity)

Thank you for your attention

QUESTIONS ?