

Applications of cryptographic identifiers in Ambient Networks

Göran Selander
Ericsson Research



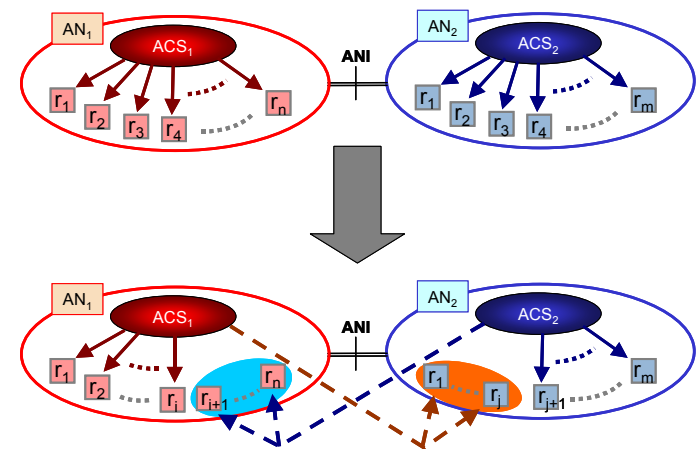
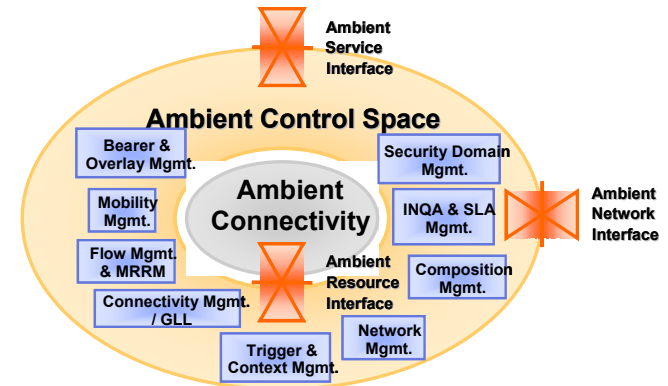
Outline

ITU-T

- o Ambient Networks
- o Cryptographic identifiers
- o Crypto IDs in Ambient Networks
- o Management and interaction scenario
- o Summary and final words

Ambient Networks

- EU IST 6FP (2004-2007, 2 phases)
- Design of "Ambient Control Space"
 - Set of control functions and interfaces in a network domain
- Ambient Control Space + connectivity network = **Ambient Network (AN)**.
- Dynamic **composition** of ANs
 - Interaction and management of resources
- Authentication and authorisation req.
 - Wide variety of scenarios → varying trust assumptios
 - High dynamicity and large changes → strong identification
 - Change of ownership/authority → delegation and revocation





ITU-T

Cryptographic Identifiers

- Public Key Crypto and digital signatures
 - Private key for signing
 - Public key for verifying signature
- Crypto ID
 - Public key is used as identifier
 - Hash(Public key) used as shorthand as in HIP
 - Unmanaged namespace
 - Self-generated public/private key-pair
 - Stochastically unique
 - Used in PGP, SSH, HIP etc.

Analogy:

- Public key → Identifier
 - Represented by a photo of a person



- Private key → Identity
 - Represented by the person itself

Rationale:

- Taking the photo requires the unique person
- Performing the signature requires the private key

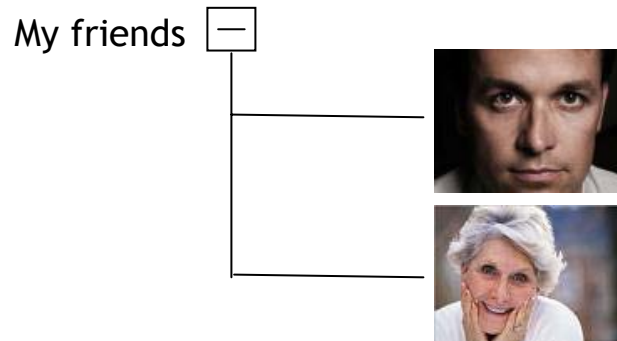
Crypto IDs can be applied in various trust relations

ITU-T

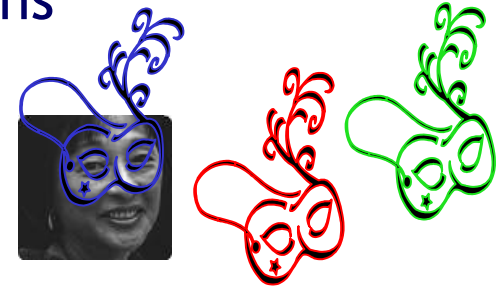
- Using crypto IDs in 'opportunistic' auth.: Entity sameness



- Pre-shared crypto ID: Trusted entities



- Ephemeral crypto IDs: Unlinkability of entity actions



- Certification of crypto ID:

- Assertion of properties



- Delegation of authority




N.B.: Combinations are possible

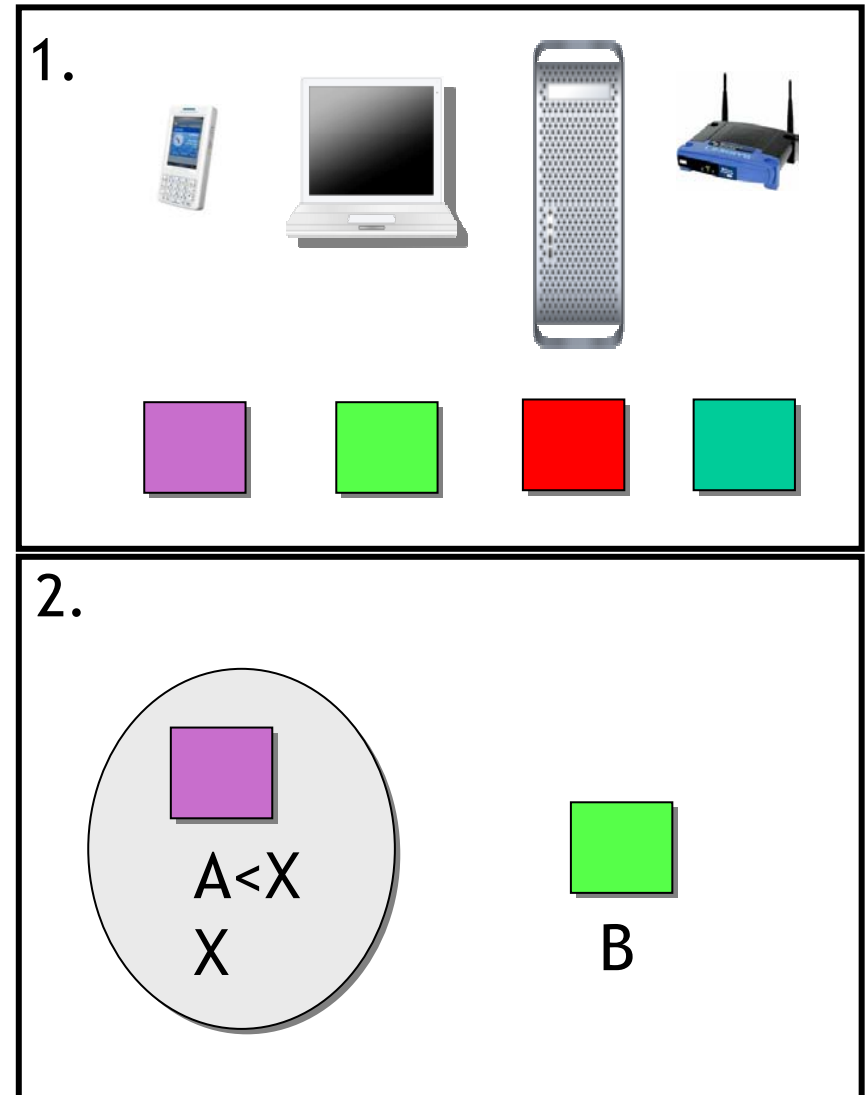


Crypto IDs in AN

ITU-T

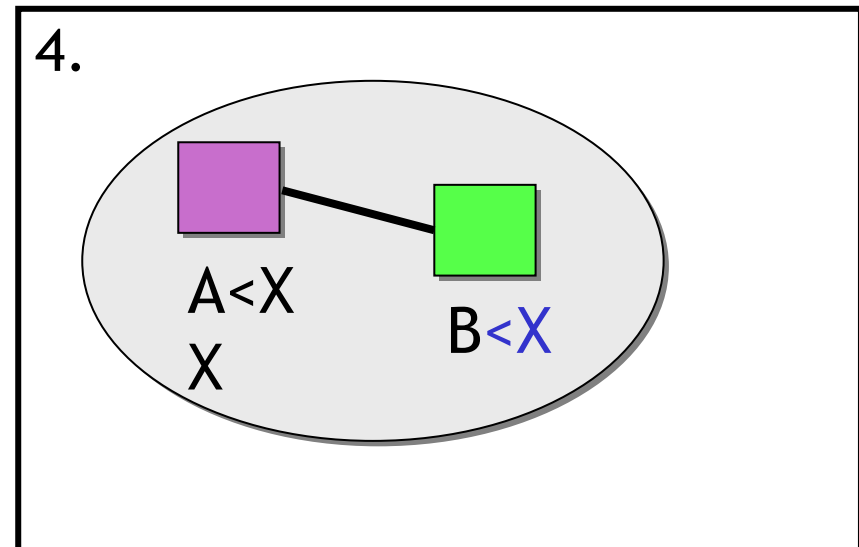
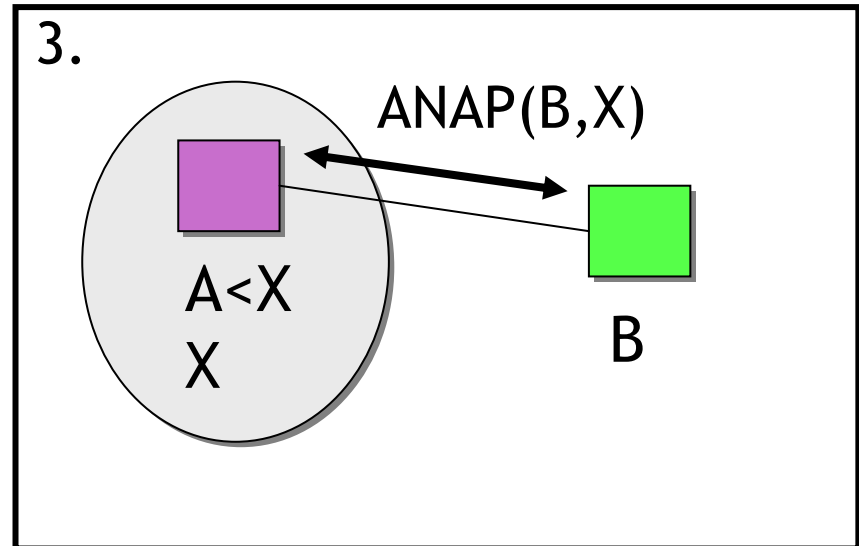
- Crypto IDs are used to identify
 - Nodes
 - Networks/domains
 - Groups of nodes with common authority
- Attachment protocol (ANAP)
 - Provides basic connectivity & security association
 - Opportunistic authentication of crypto network IDs
 - Additional authentication hooks (optional)
 - Native or carried on top of different legacy protocols
 - Selection of common protocol also in scope
- Crypto IDs also used for authorisation
 - Network membership certificates
 - Access control policies within or between networks
 - Delegation between nodes and/or networks
- Convention: Use same identifier for the authority/manager as the network it manages

- o Installation procedure
 - Make node AN aware
 - With or w/o manager functionality
- o Notation
 - Capitals for crypto IDs
 - A, B, C, ...
 - Listed under physical host
 - Hosts private key
 - Relations between entities
 - Member, Peer, Delegate
- o Fig 2
 - AN aware nodes A and B
 - Node A member of AN X
 - Manager X hosted in 



AN Configuration Management

- Configuration procedure
 - Enroll nodes in AN
- Node-network auth
- Authentication alternatives
 - Manual authentication
 - Pre-installed crypto Ids
 - TTP-assisted
- Mutual authorisation
 - X authz B as member
 - Issue membership cert
 - B authz X as manager
 - Install network policies





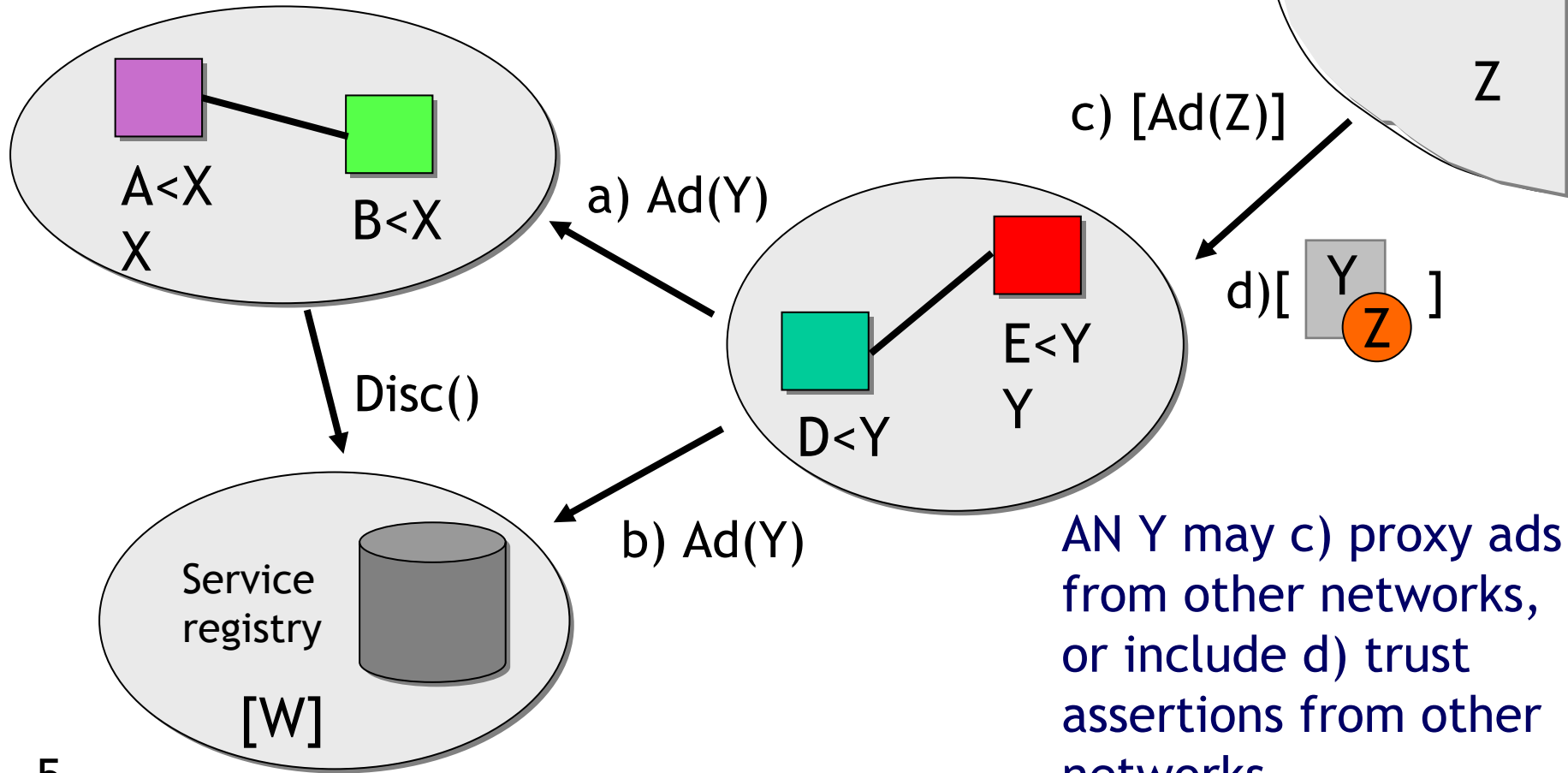
ITU-T

AN Advertisements

- Network advertisements in reserved parts of legacy access technology broadcast messages
 - E.g. beacons
 - General ads
- Network advertisements in ANAP or after attachment
 - Directed ads
- Advertisement may contain
 - Crypto IDs
 - Signatures
 - Trusted assertions
- Enables verification of advertisement from trusted sources
- Enables listening mode without revealing presence

AN Advertisement & Discovery

AN Y advertise network services a) directly, or b) via intermediate service registry.



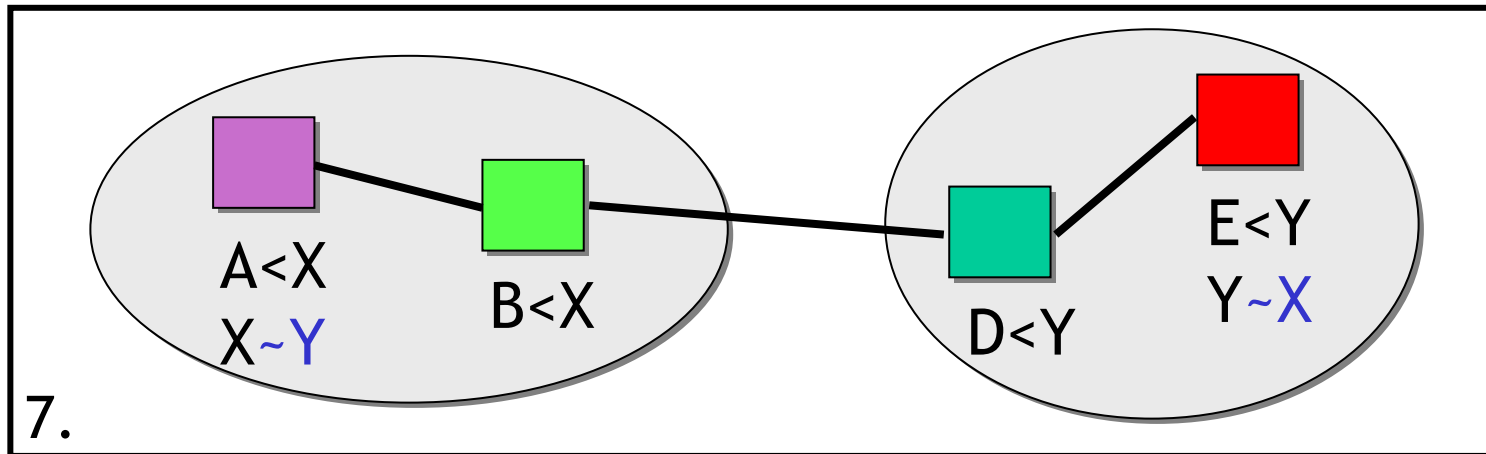
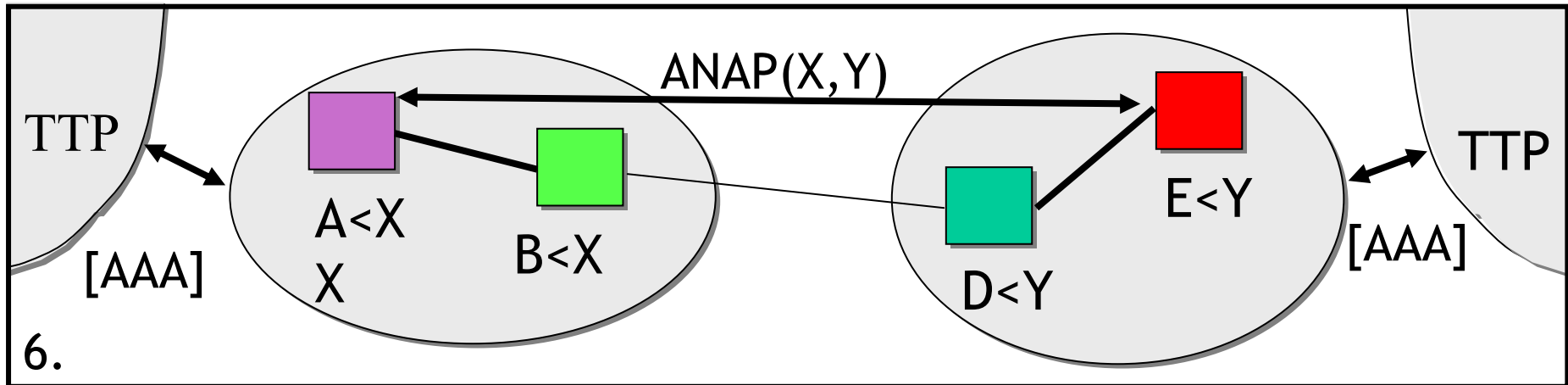
AN Y may c) proxy ads from other networks, or include d) trust assertions from other networks.

[] = optional

5.

AN Attachment

ITU-T Network-network attachment enables composition negotiation & subsequent service provisioning/resource sharing





ITU-T

Summary

- Crypto IDs identifying nodes and networks
- Secures communication between nodes and networks
- Secures configuration of networks, network attachment & negotiation of new services
- Enables verification of advertisement from trusted sources
- Enables listening mode without revealing presence
- Enables unlinkability of end-network actions
- Enables delegation of authority

Final words; conjecture

Cryptographic network identifiers
will be an important component
of a future digital identity