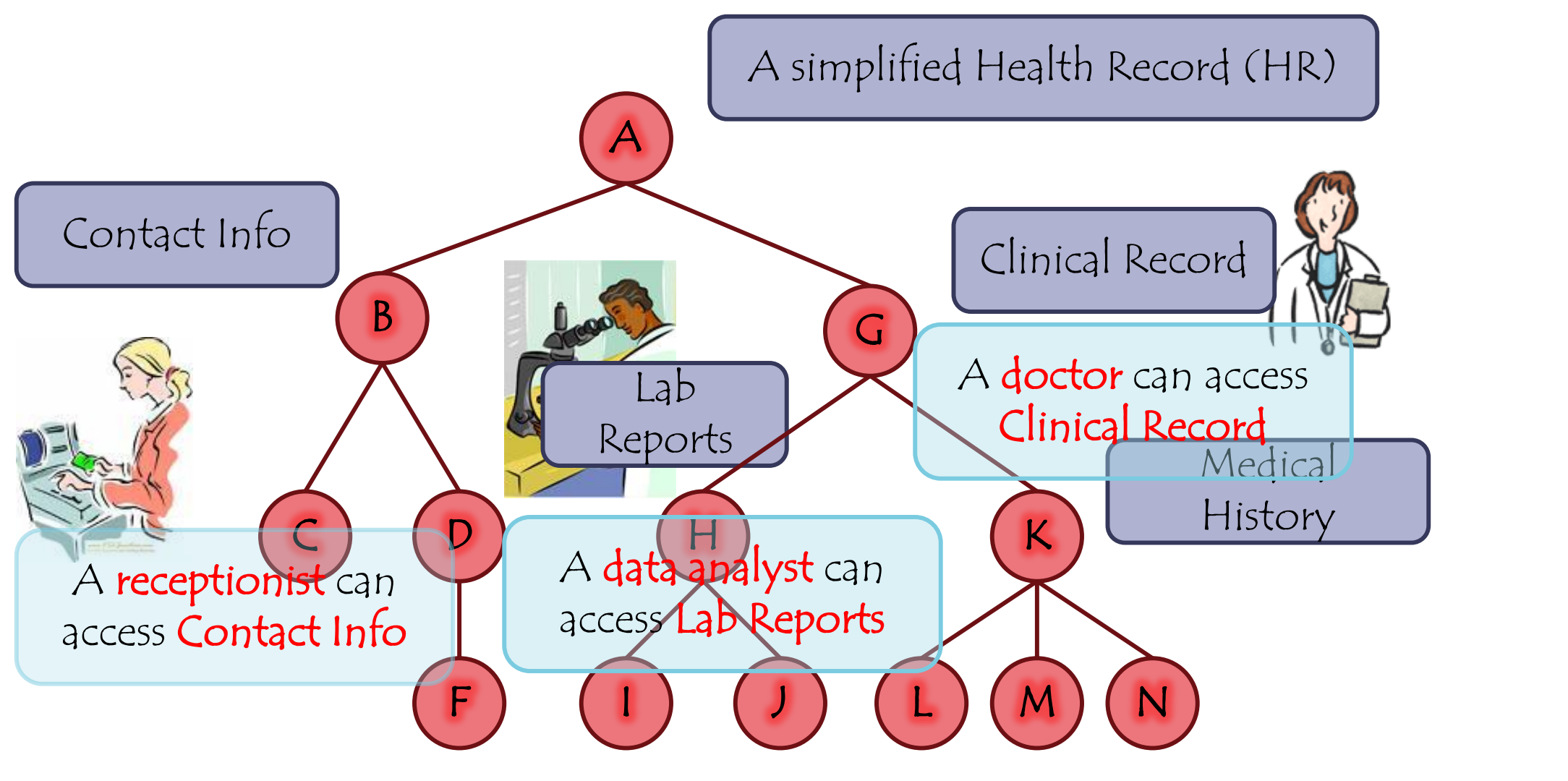
CERIAS

the center for education and research in information assurance and security

Preserving Privacy in Policy-Based Content Dissemination

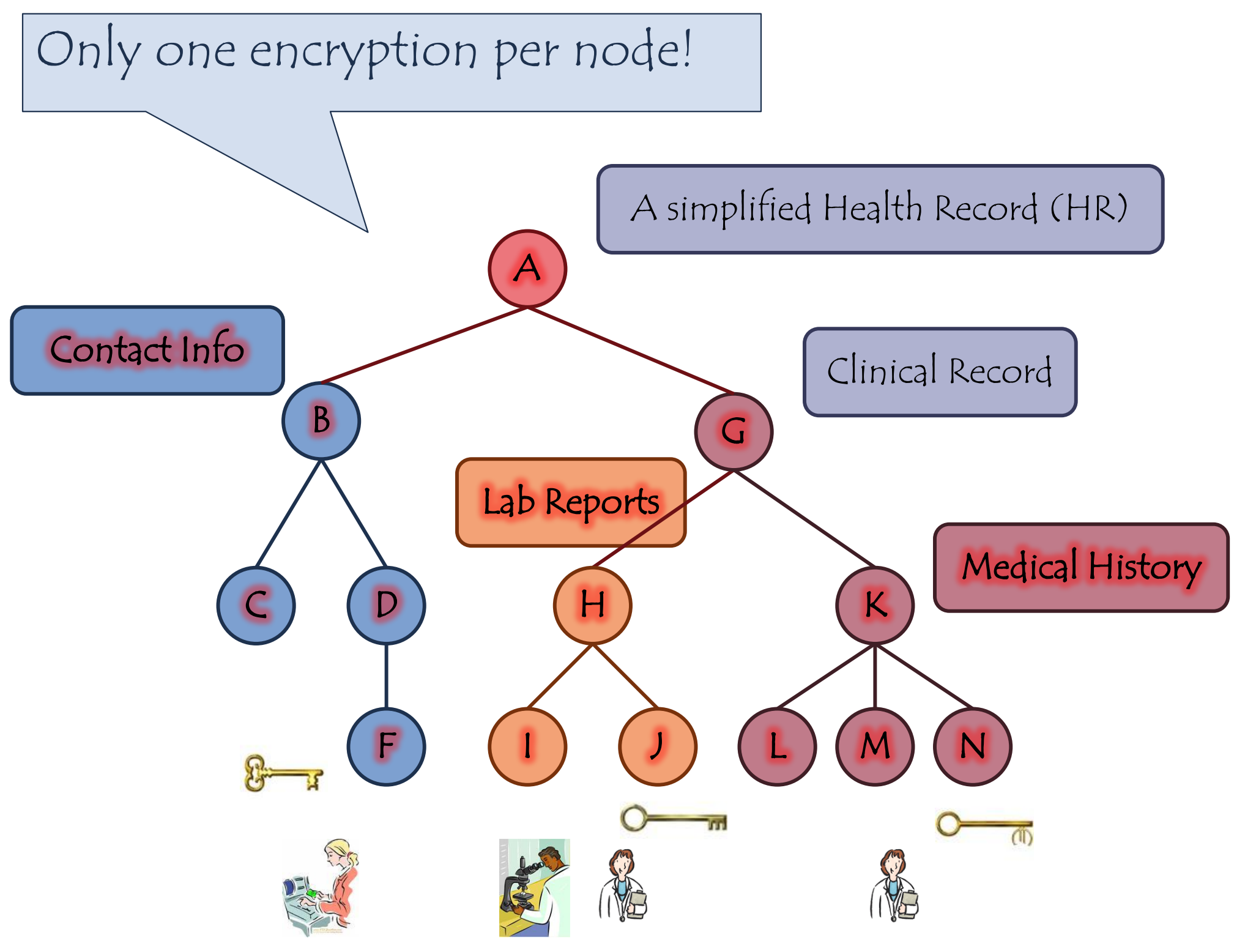
Mohamed Nabeel, Ning Shang, Elisa Bertino (Purdue University)

What is policy based content dissemination?

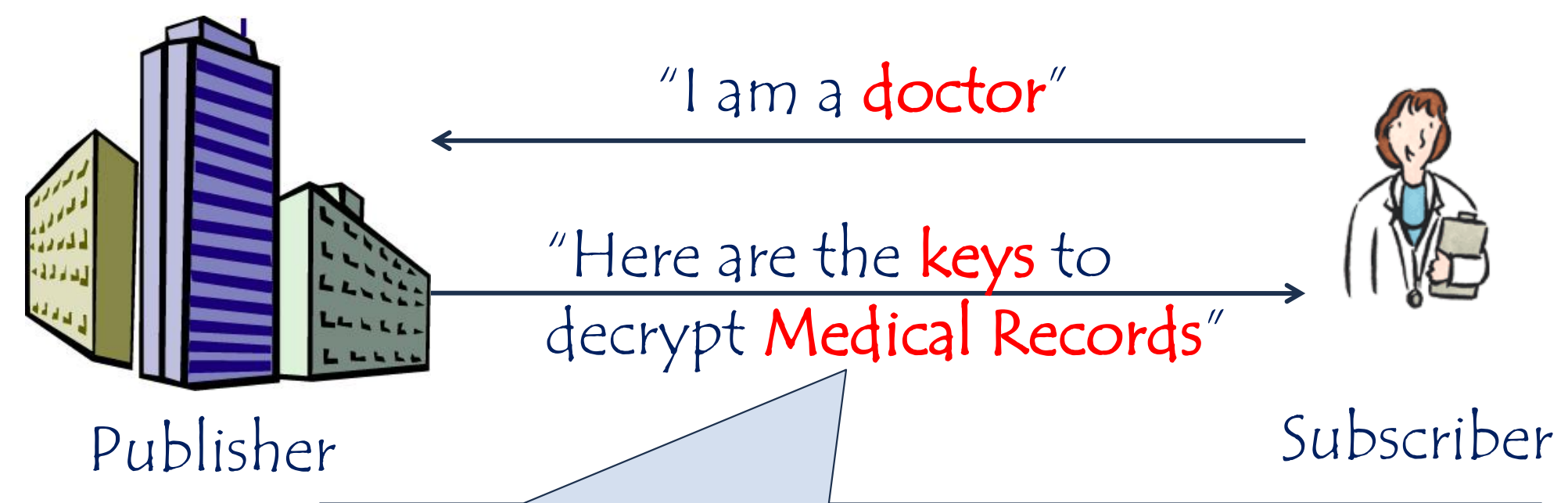

A simplified Health Record (HR)
A
B
G
C
D
H
K
F
I
J
L
M
N
Contact Info
Lab Reports
Clinical Record
Medical History
A receptionist can access Contact Info
A data analyst can access Lab Reports
A doctor can access Clinical Record

Attribute Based Access Control (ABAC)

A simplistic approach using encryption



Issue #1: Privacy of the users is not preserved

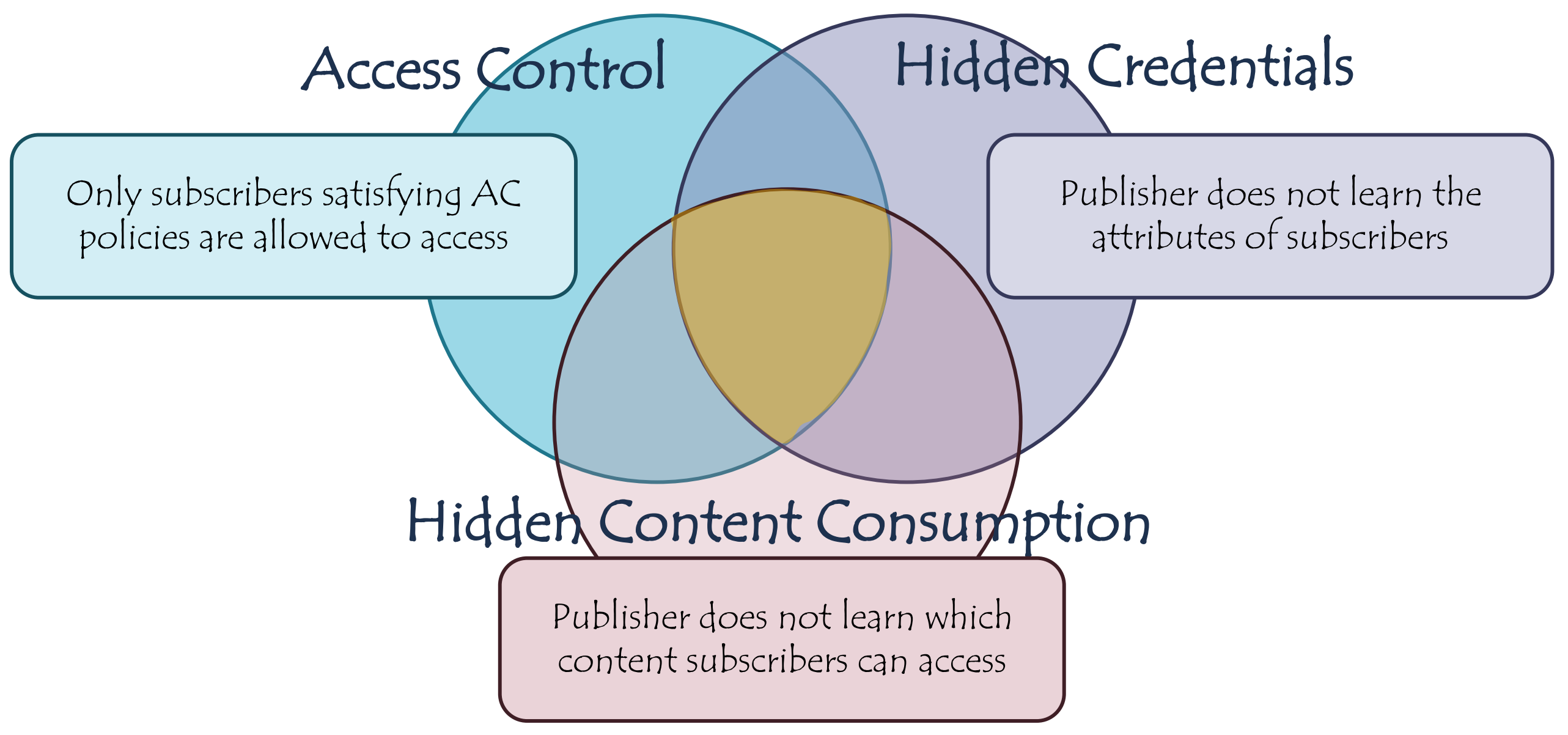


1. Need to reveal credentials
2. Need a private communication channel for re-keying

Issue #2: The key management does not scale

Re-keying has O(n) communication overhead (n = number of users)

Requirements for maximal amount of privacy & security



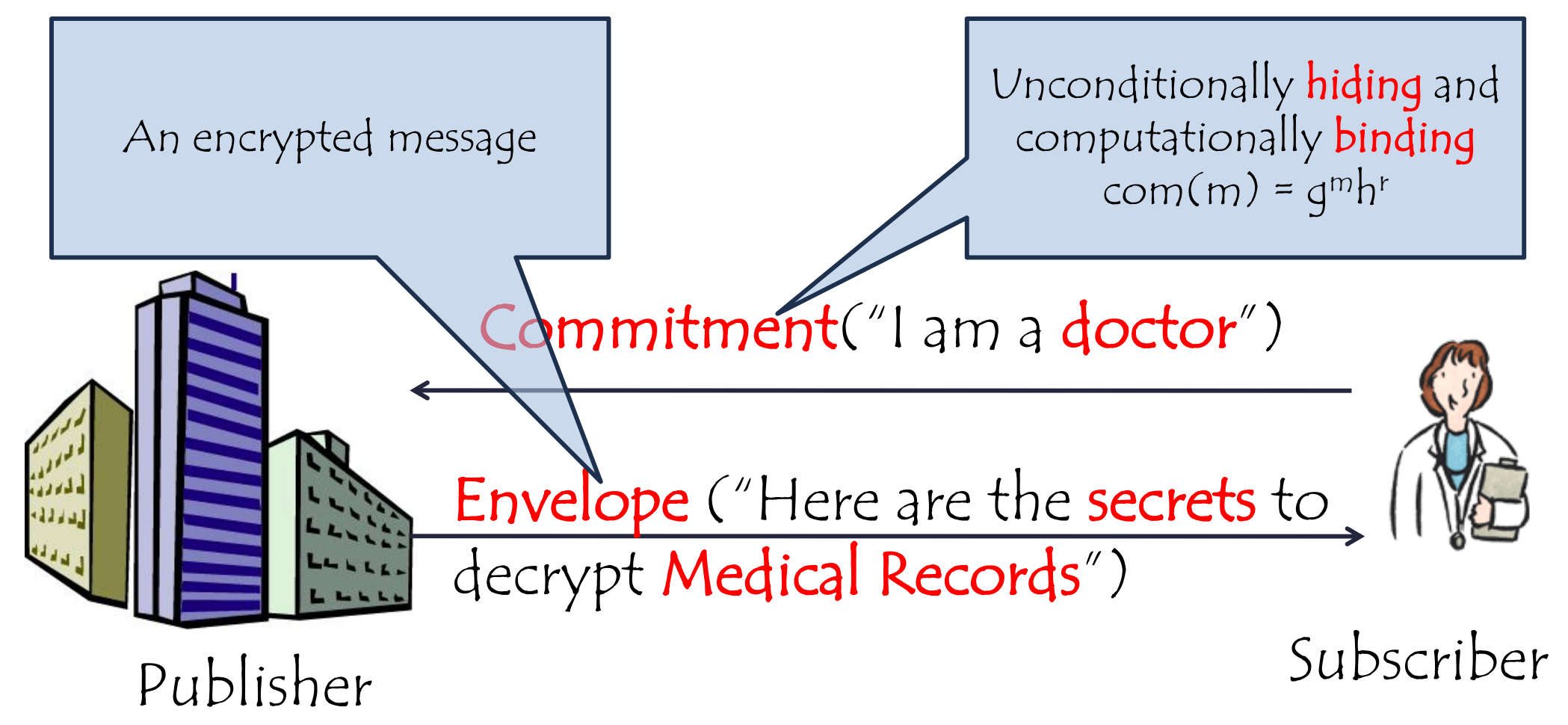
Only subscribers satisfying AC policies are allowed to access

Publisher does not learn the attributes of subscribers

Publisher does not learn which content subscribers can access

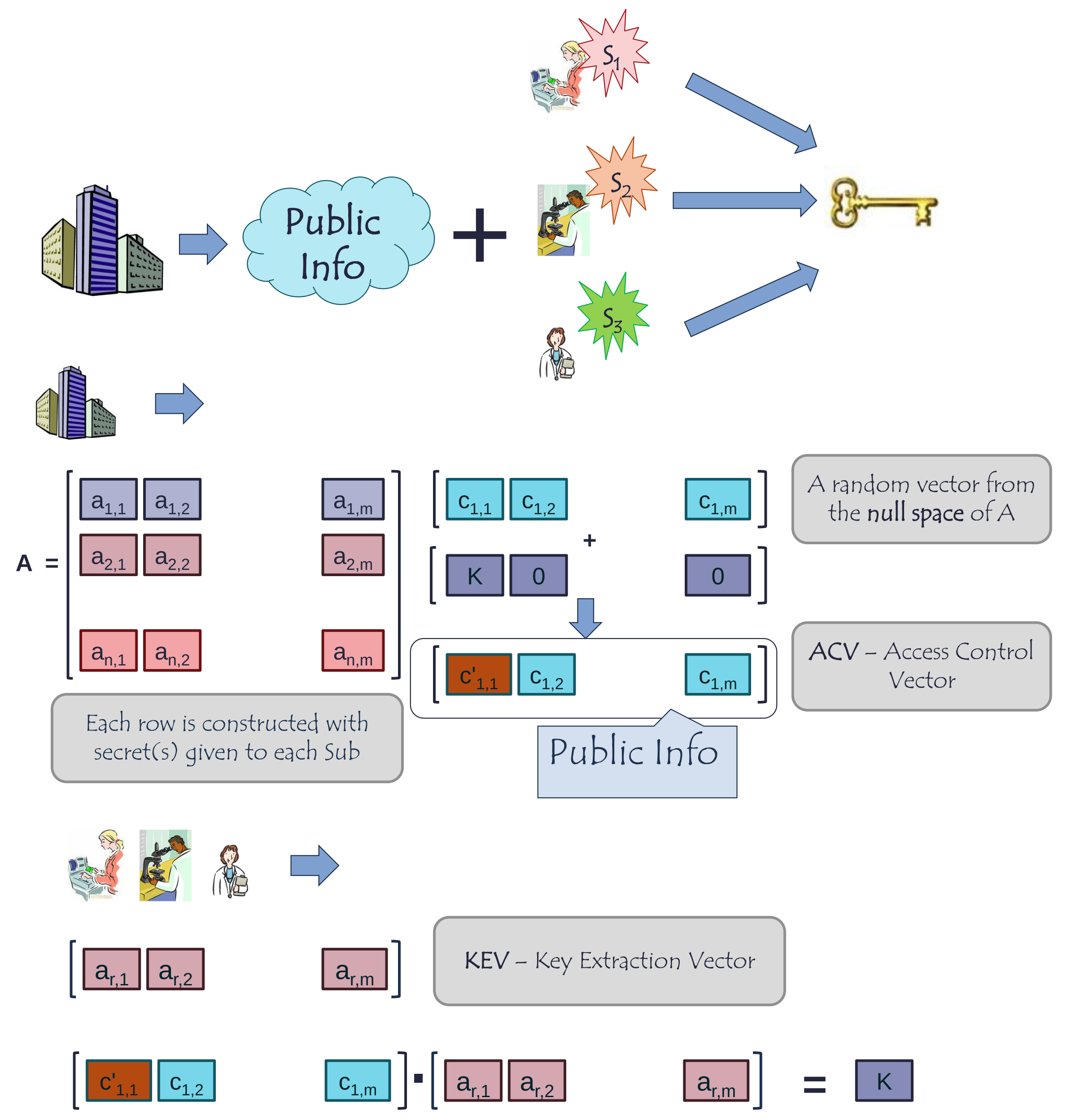
Building blocks: OCBE and BGKM schemes

OCBE: Oblivious Commitment Based Envelope


An encrypted message
Unconditionally hiding and computationally binding com(m) = $g^m h^r$
Commitment("I am a doctor")
Envelope ("Here are the secrets to decrypt Medical Records")
Publisher
Subscriber

- Publisher does not learn credentials
- User can open the envelope only if her credential satisfies the condition

BGKM: Broadcast Group Key Management


Public Info
+
S_1
S_2
S_3
A =
$a_{1,1}$ $a_{1,2}$ $a_{1,m}$
$a_{2,1}$ $a_{2,2}$ $a_{2,m}$
$a_{n,1}$ $a_{n,2}$ $a_{n,m}$
$c_{1,1}$ $c_{1,2}$ $c_{1,m}$
+
K 0 0
$c'_{1,1}$ $c_{1,2}$ $c_{1,m}$
Public Info
$a_{r,1}$ $a_{r,2}$ $a_{r,m}$
$c'_{1,1}$ $c_{1,2}$ $c_{1,m}$ · $a_{r,1}$ $a_{r,2}$ $a_{r,m}$ = K

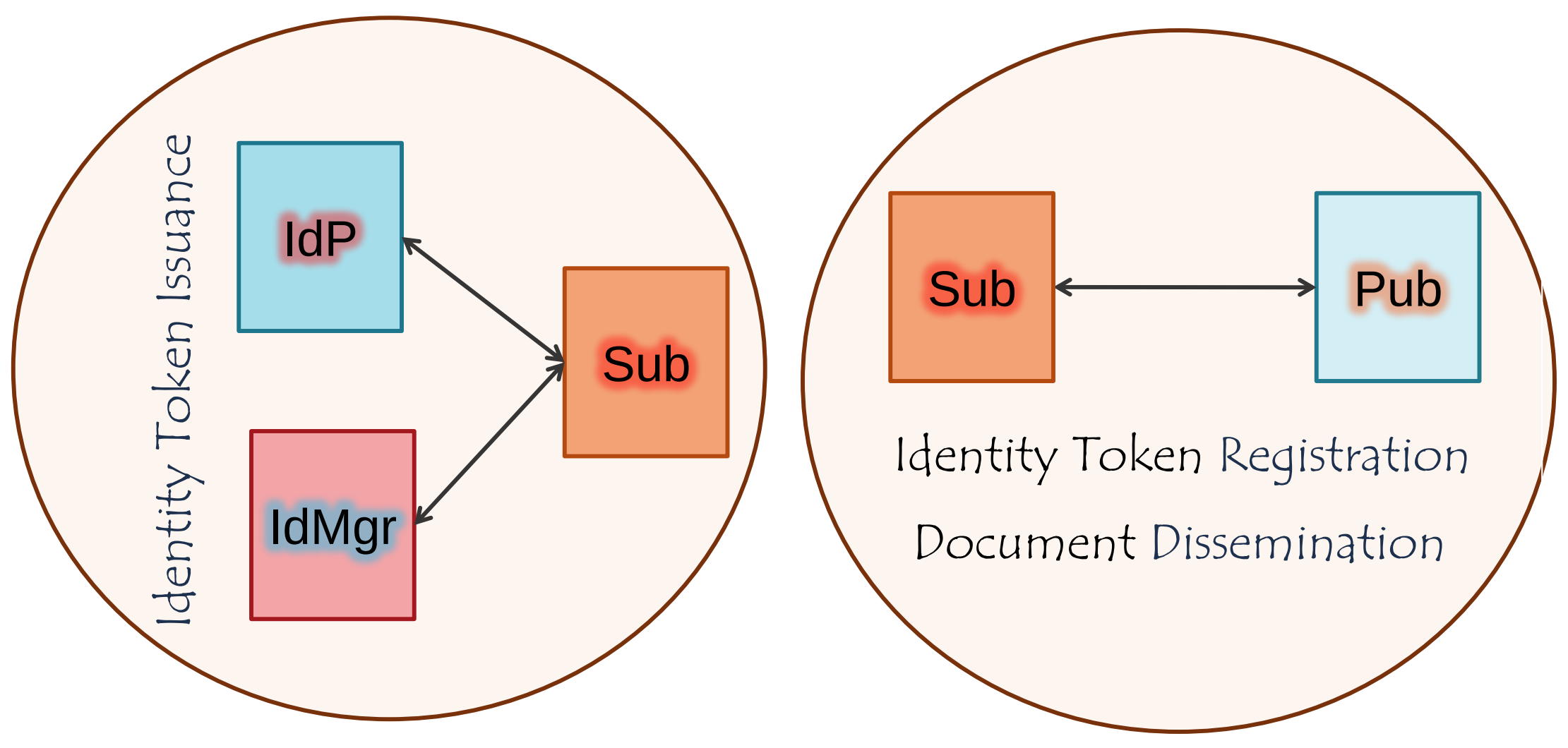
A random vector from the null space of A

ACV – Access Control Vector

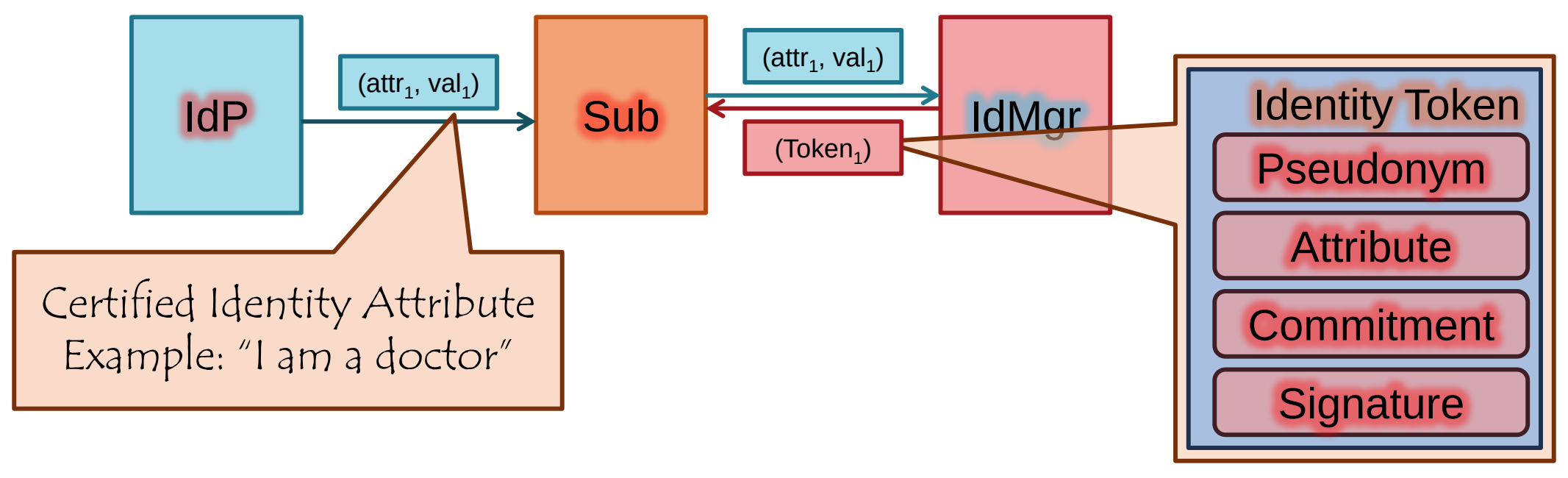
Each row is constructed with secret(s) given to each Sub

KEV – Key Extraction Vector

Putting everything together (OCBE + BGKM)

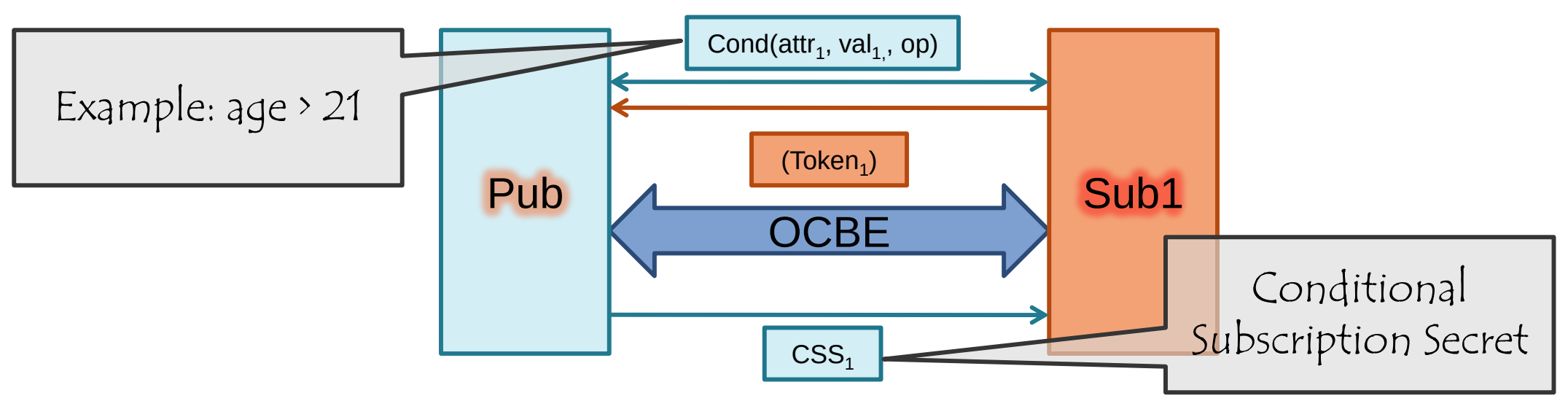


Identity Token Issuance

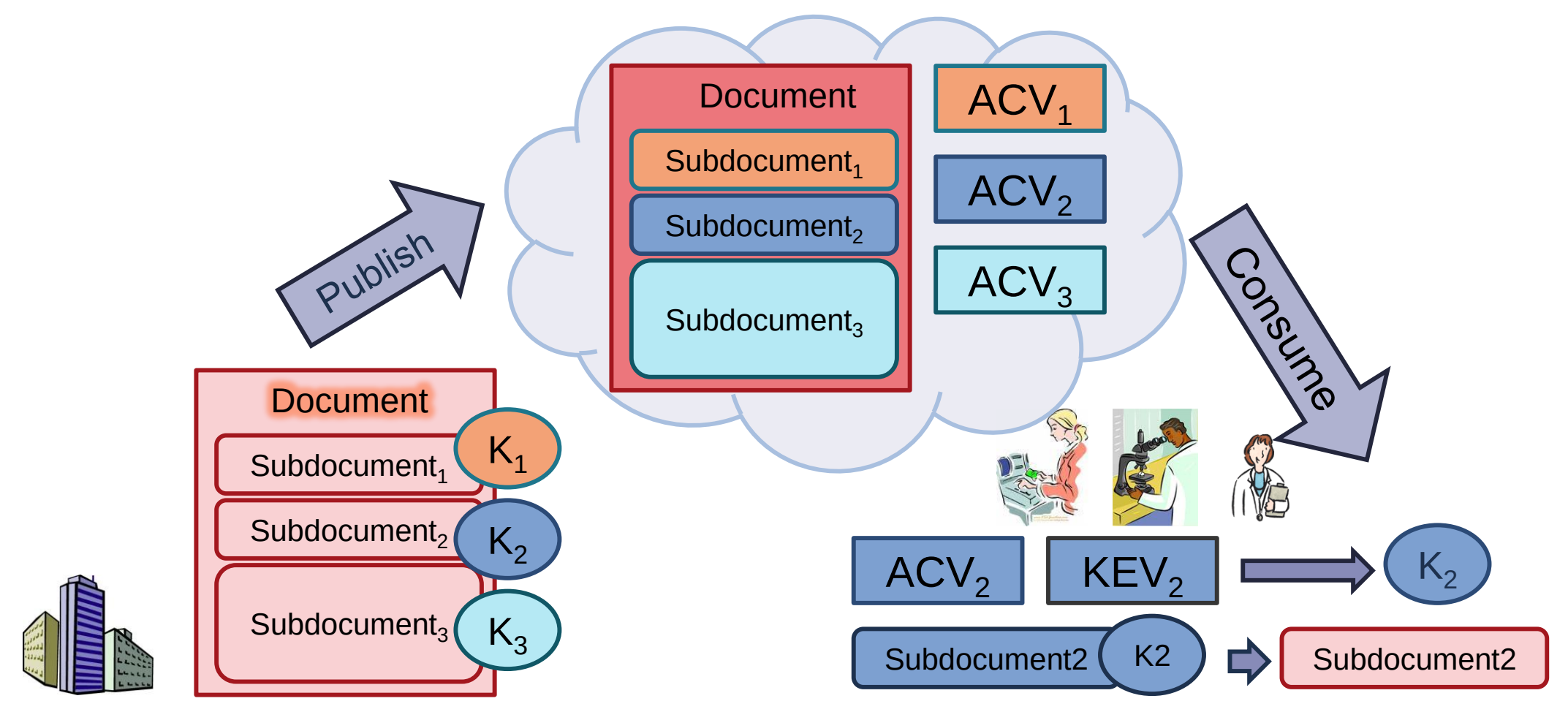


Certified Identity Attribute Example: "I am a doctor"

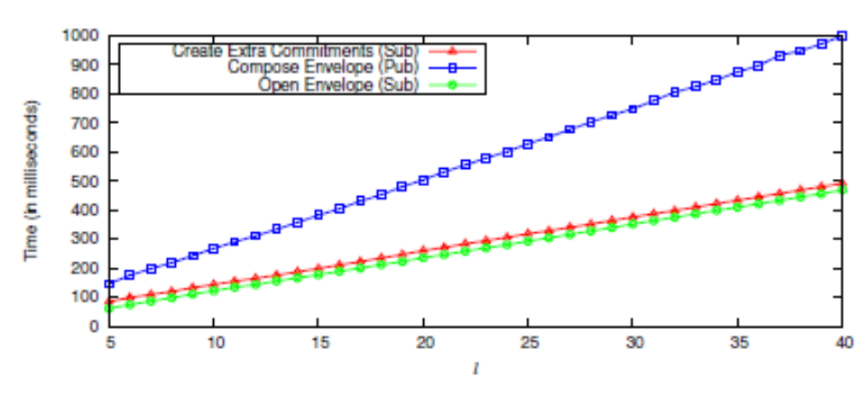
Identity Token Registration



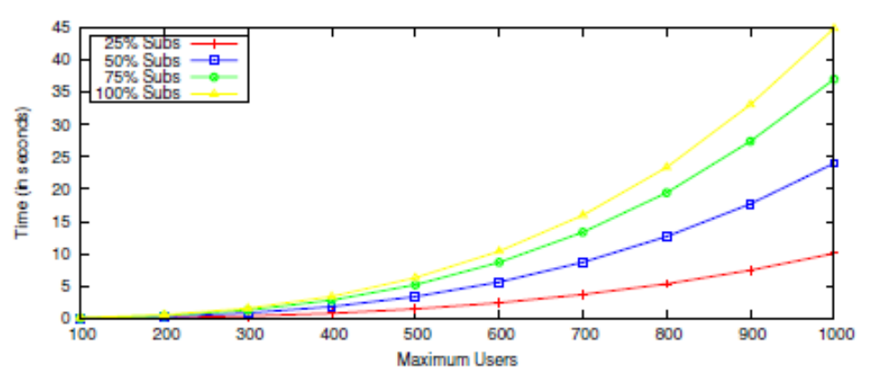
Document Dissemination



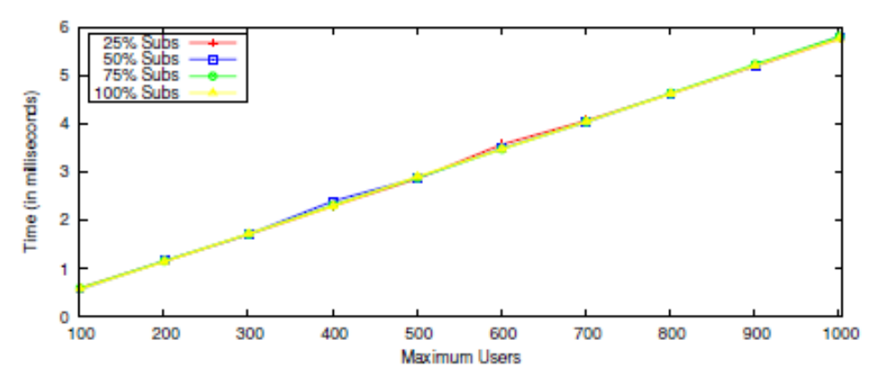
Some selected experimental results



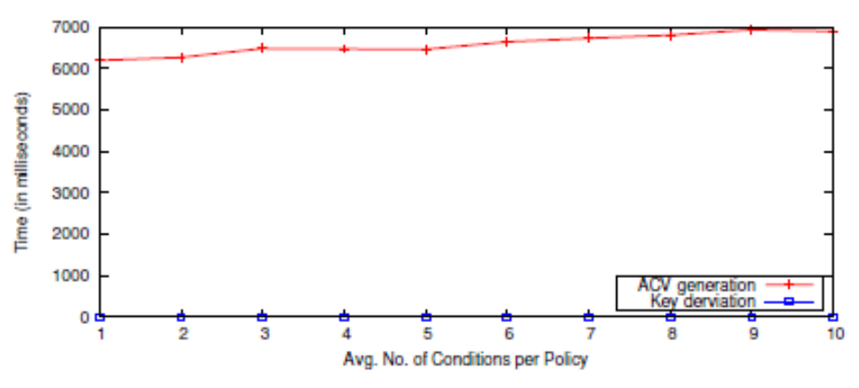
Average computation time for running one round of GE-OCBE protocol



Time to generate an ACV for different user configurations



Key derivation time for different user configurations



ACV generation and key derivation for different number of conditions per policy

PURDUE UNIVERSITY

CERIAS®

Discovery Park e-Enterprise Center