

# REDUCING THE COMPUTATIONAL COST OF CERTIFICATION PATH VALIDATION IN MOBILE PAYMENT

Cristina Satizábal<sup>1,2</sup>, Rafael Martínez-Peláez<sup>1</sup>, **Jordi Forné**<sup>1</sup>, Francisco Rico-Novella<sup>1</sup>

<sup>1</sup>Universitat Politècnica de Catalunya (Spain)

<sup>2</sup>Universidad de Pamplona (Colombia)





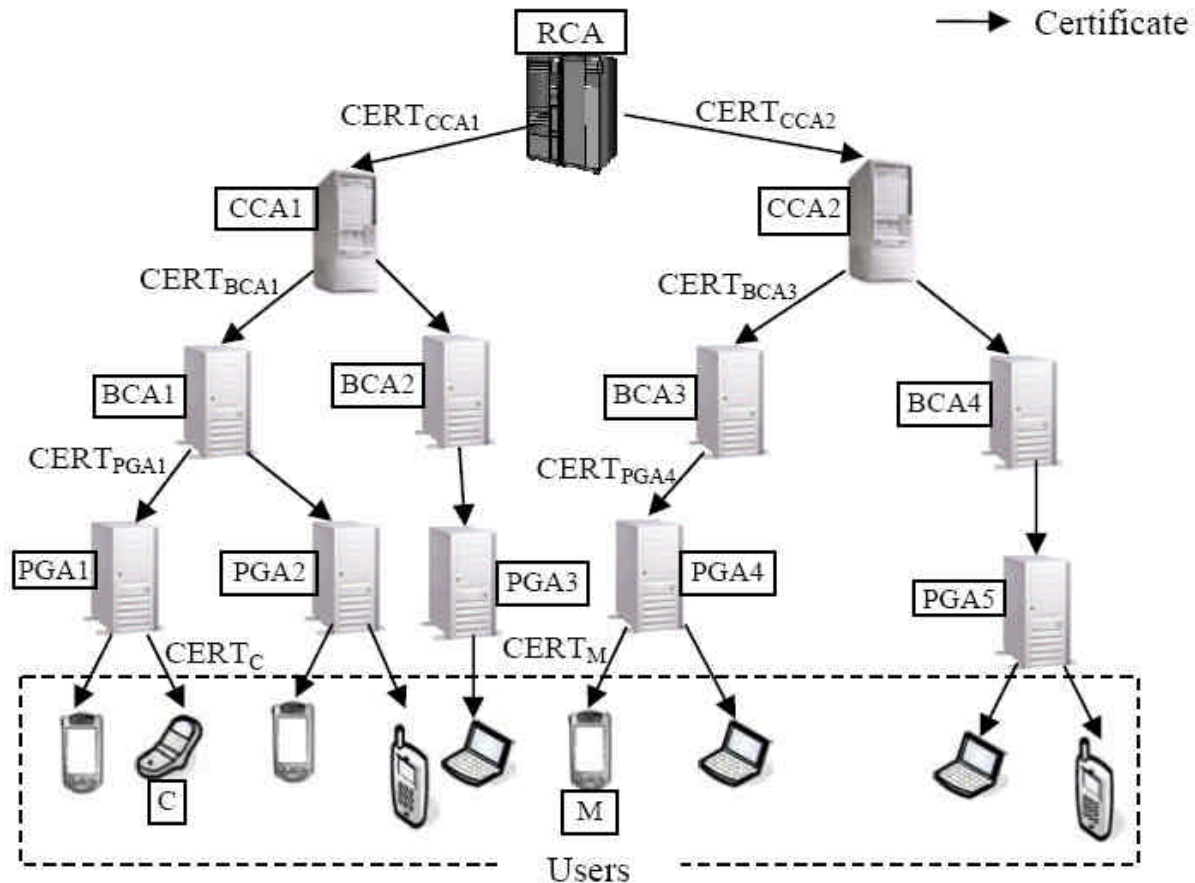
# INTRODUCTION

---

- **M-PAYMENT:**

- Exchange of money using mobile devices
- Strong security requirements
- Constrained devices (PDAs, mobile phones)
  - Computational power
  - Battery
  - Storage capability

# SCENARIO



Hierarchical PKI for P2P m-payment



# PROBLEM

---

**PKI Grows**

**Many CAs**

**TRUST CHAINS = CERTIFICATION PATHS**

**VALIDATION**

**CONSTRAINED DEVICES**



# PROBLEM

---

- **CERTIFICATION PATH VALIDATION**

- Discovering the certification path
- Retrieving the certificates
- **Verifying the digital signatures**
- Checking the revocation status of the certificates

- *Problems:*

- Complexity of the process
- Storage and processing capacities of mobile devices



# MAIN IDEA

---

- **VALIDATION OF INFORMATION**
  - Through digital signature
    - With the public key of the signer
    - Validation requires “costly” public key operations
  - Through hash functions
    - With a shared secret (example: H-MAC)
    - Validation does not require PK operations
- Can we generate a credential that allows both validation approaches?



# PROPOSED SOLUTION: TRUTHC

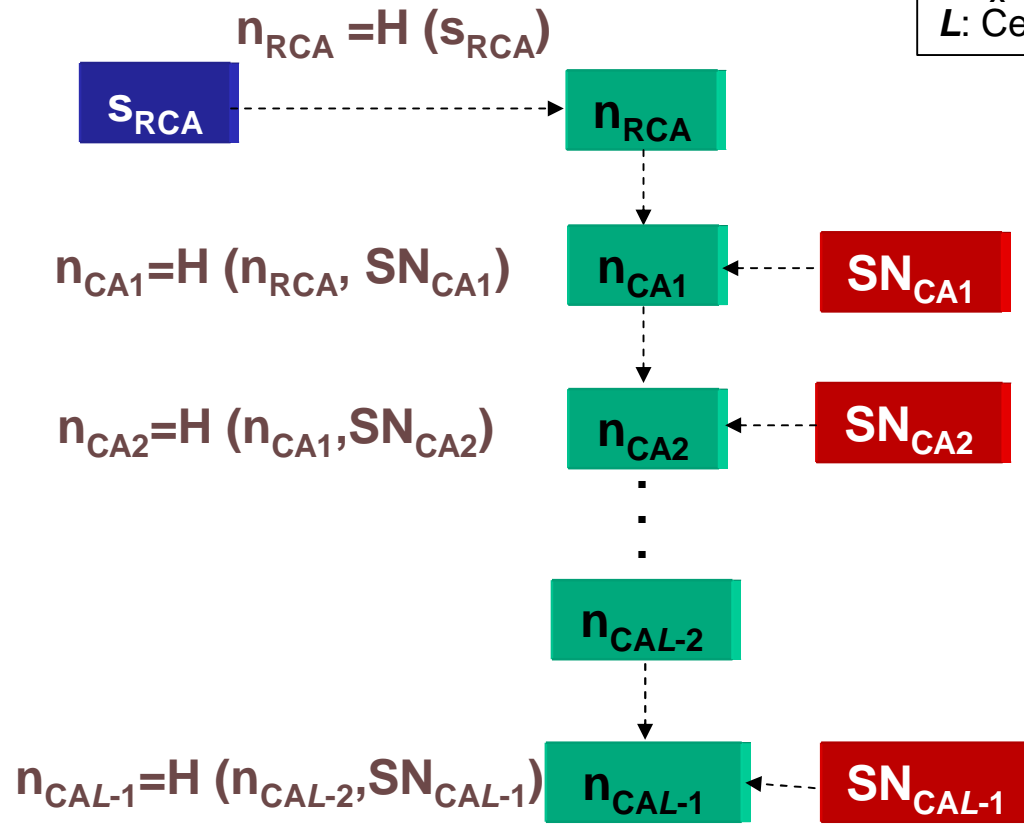
---

- **TRUTHC (Trust Relationship Using Two Hash Chains)**
  - Hash chains to establish trust relationship among the entities of a hierarchical PKI => Only hash operations in path validation
  - Reduces number of public key encryption operations => less computational cost => less processing capacity
  - Reduces complexity of certification path validation
  - Price to pay: Validation requires the knowledge of a secret

# TRUTHC DESCRIPTION

## SECRET SEEDS' CHAIN

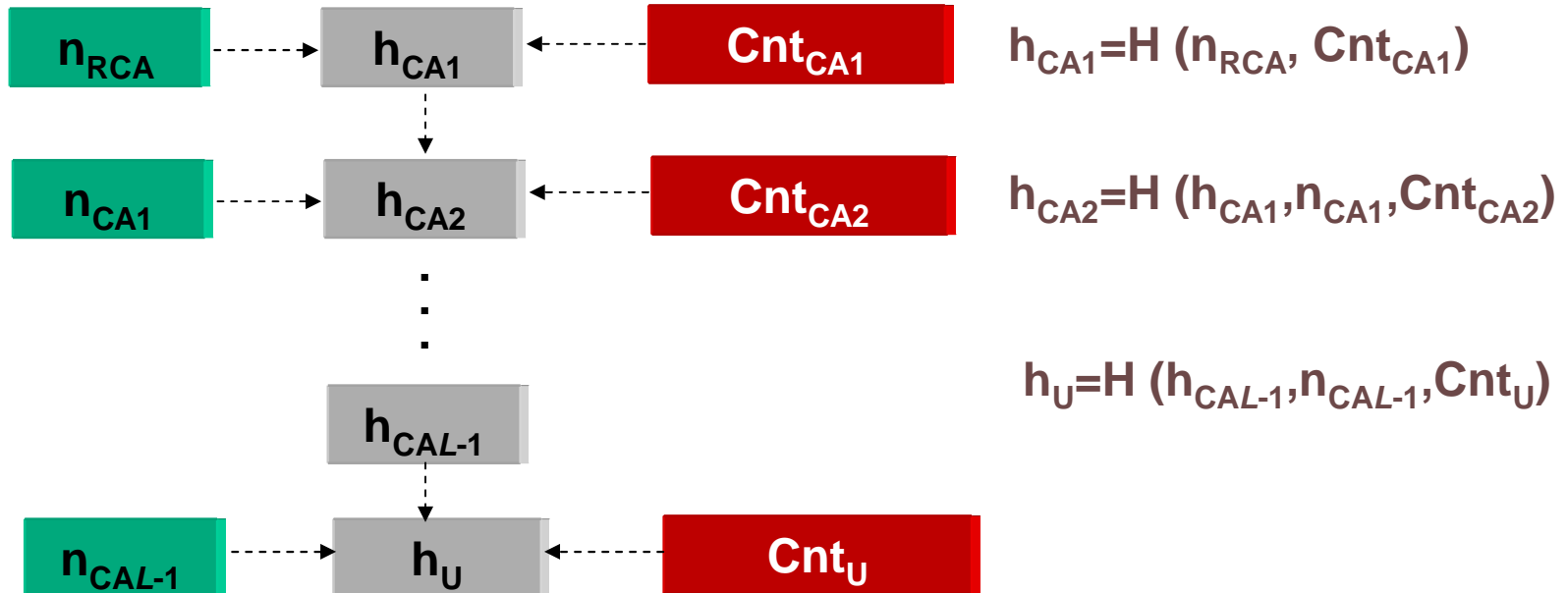
$s_{RCA}$ : Random secret seed  
 $n_x$ : Secret seed of authority X  
 $SN_x$ : Serial number of  $CERT_x$   
 $L$ : Certification path length



# TRUTHC DESCRIPTION

## ■ INTEGRITY CHECK VALUES' CHAIN

$n_x$ : Secret seed of authority X  
 $h_x$ : Integrity check value of entity X  
 $\text{Cnt}_x$ : Content of  $\text{CERT}_x$   
 $L$ : Certification path length



# TRUTHC DESCRIPTION

## ISSUING PROCESS

$CERT_X$ : Certificate of entity X  
 $s_{RCA}$ : Random secret seed  
 $n_X$ : Secret seed of authority X  
 $h_X$ : Integrity check value of entity X  
 $N_X$ : Encapsulated seed of authority X  
 $PK_X$ : Public key of entity X  
 $SK_X$ : Private key of entity X

RCA

CA1

U

Issues  $CERT_{RCA}$

Chooses  $s_{RCA}$

Computes:

$n_{RCA} = H(s_{RCA})$

Issues  $CERT_{CA1}$

Computes:

$h_{CA1} = H(n_{RCA}, Cnt_{CA1})$

$n_{CA1} = H(n_{RCA}, SN_{CA1})$

$N_{CA1} = \{n_{CA1}\}_{PK_{CA1}}$

$CERT_{RCA},$   
 $CERT_{CA1},$   
 $h_{CA1}, N_{CA1}$

Computes:

$n_{CA1} = \{N_{CA1}\}_{SK_{CA1}}$

Issues  $CERT_U$

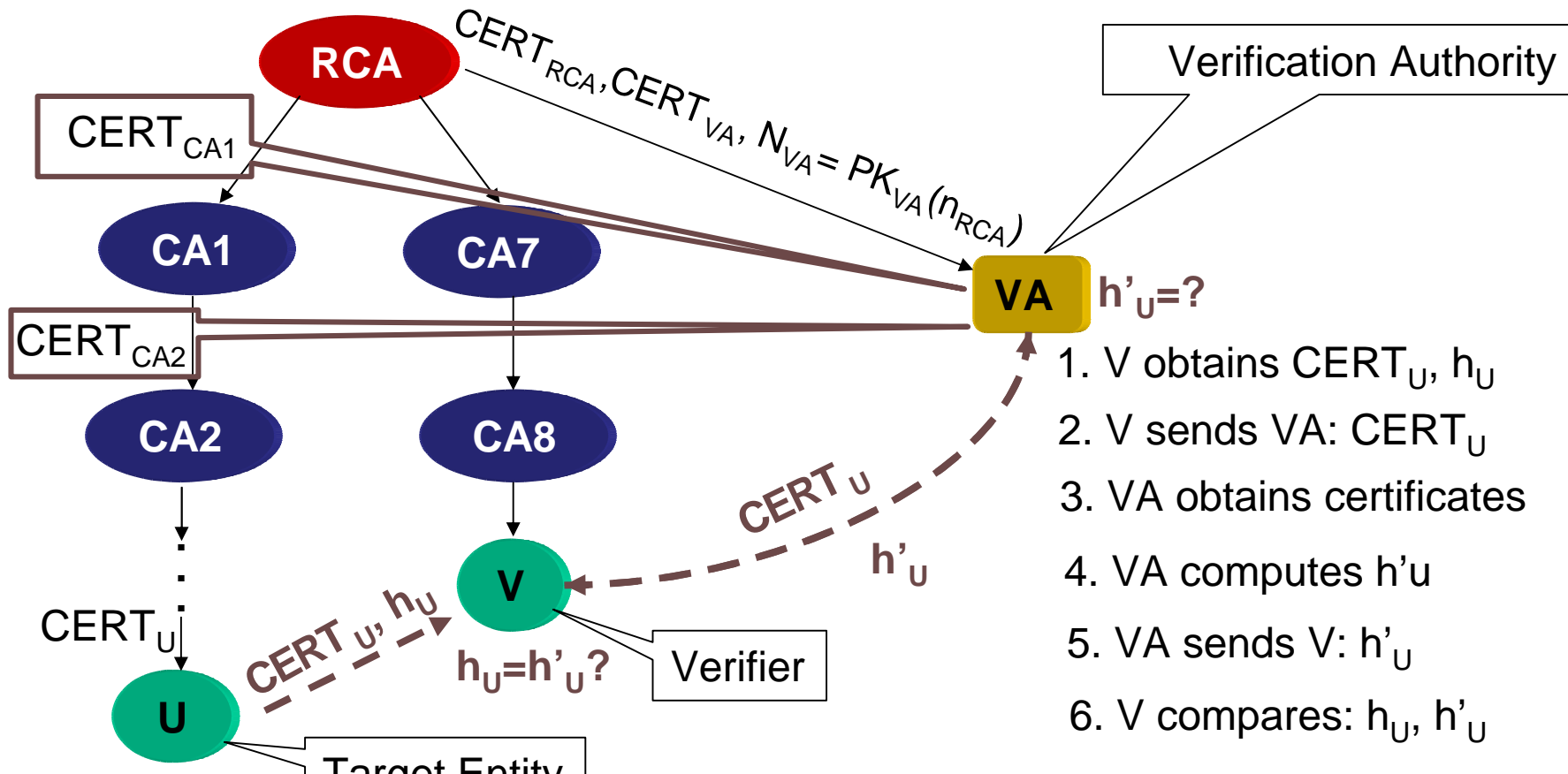
Computes:

$h_U = H(h_{CA1}, n_{CA1}, Cnt_U)$

$CERT_{RCA},$   
 $CERT_U, h_U$

# TRUTHC DESCRIPTION

## ■ VERIFICATION PROCESS





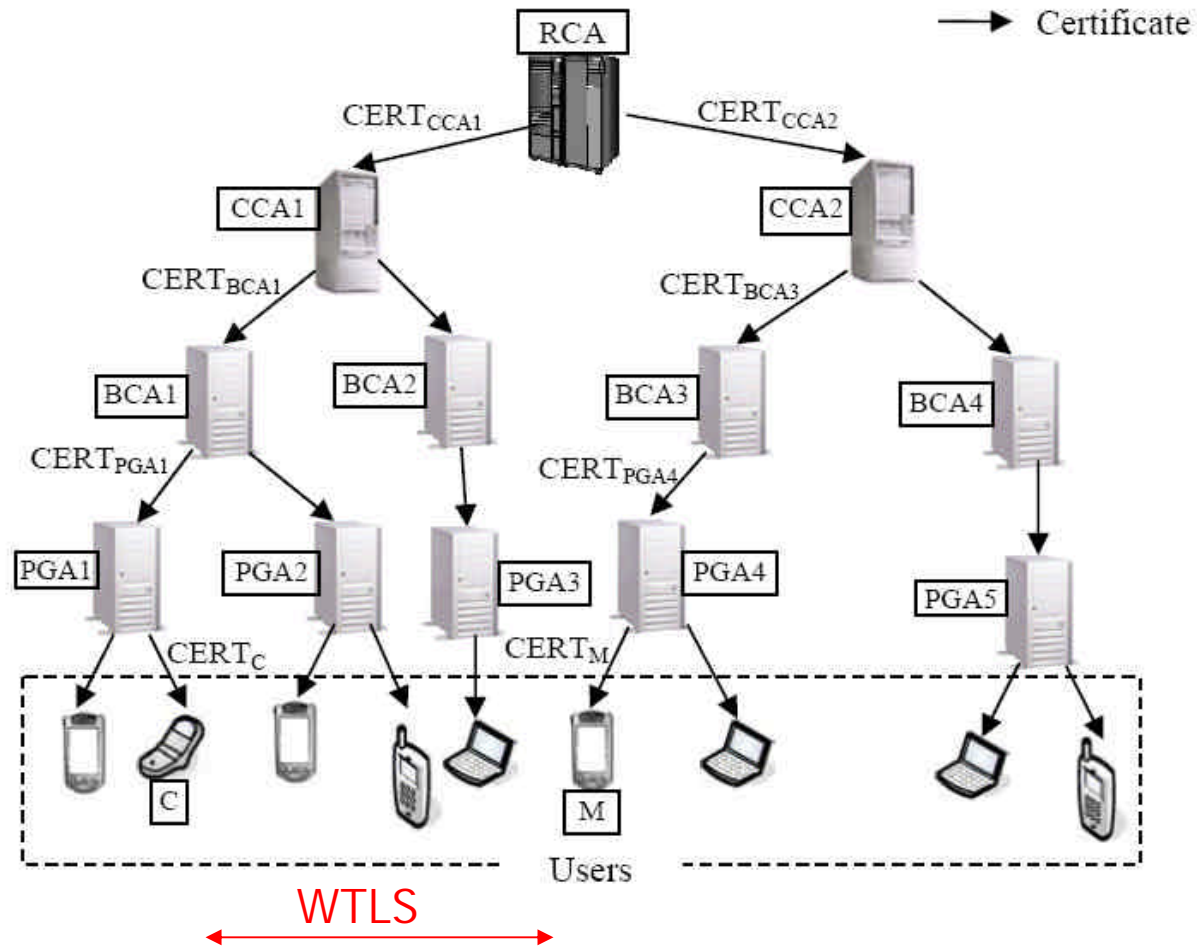
# EVALUATION SCENARIO

---

## ■ Mutual Authentication using WTLS

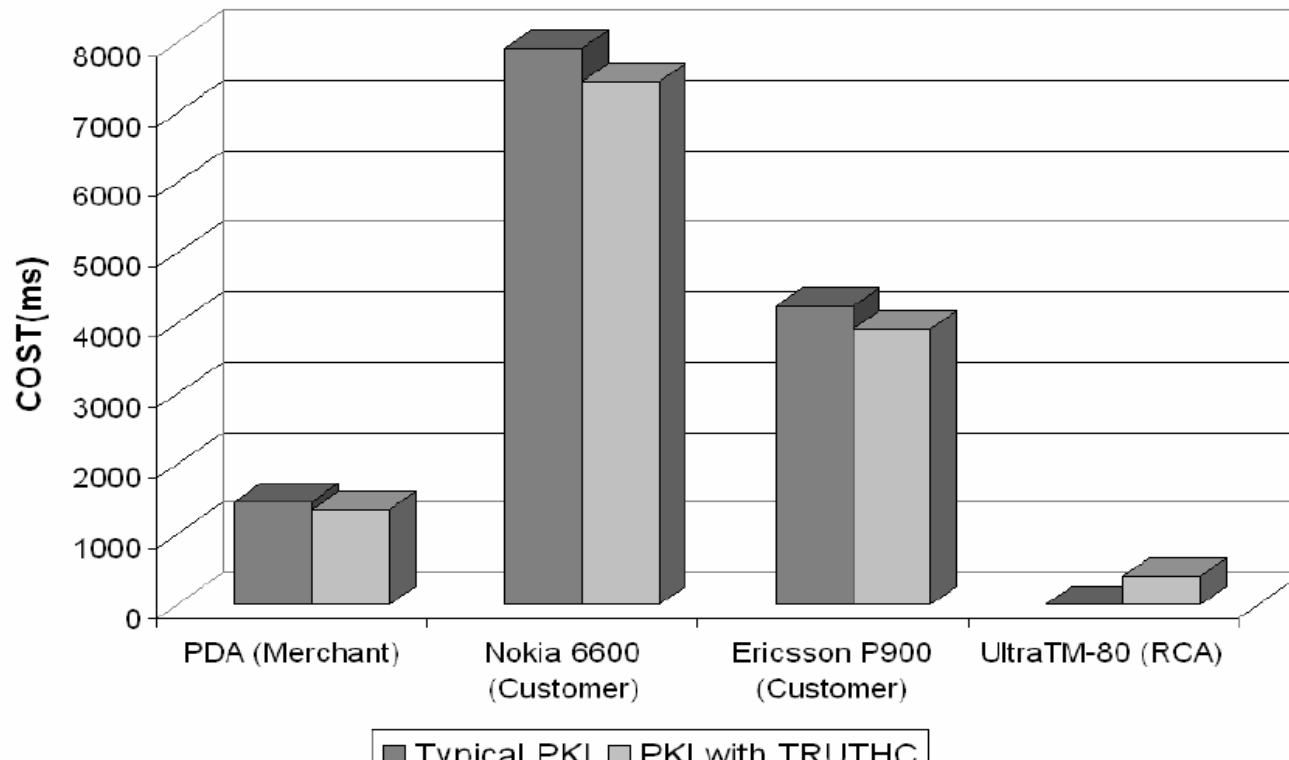
- Analyze de different type of crypto operations for each party when executing the WTLS handshake protocol.
- Apply published benchmarks for customers, merchants and the VA:
  - Customers (mobiles phones)
  - Merchant (PDA)
  - VA (workstation)
- Compare RSA-1937 vs. ECDSA-191

# EVALUATION SCENARIO



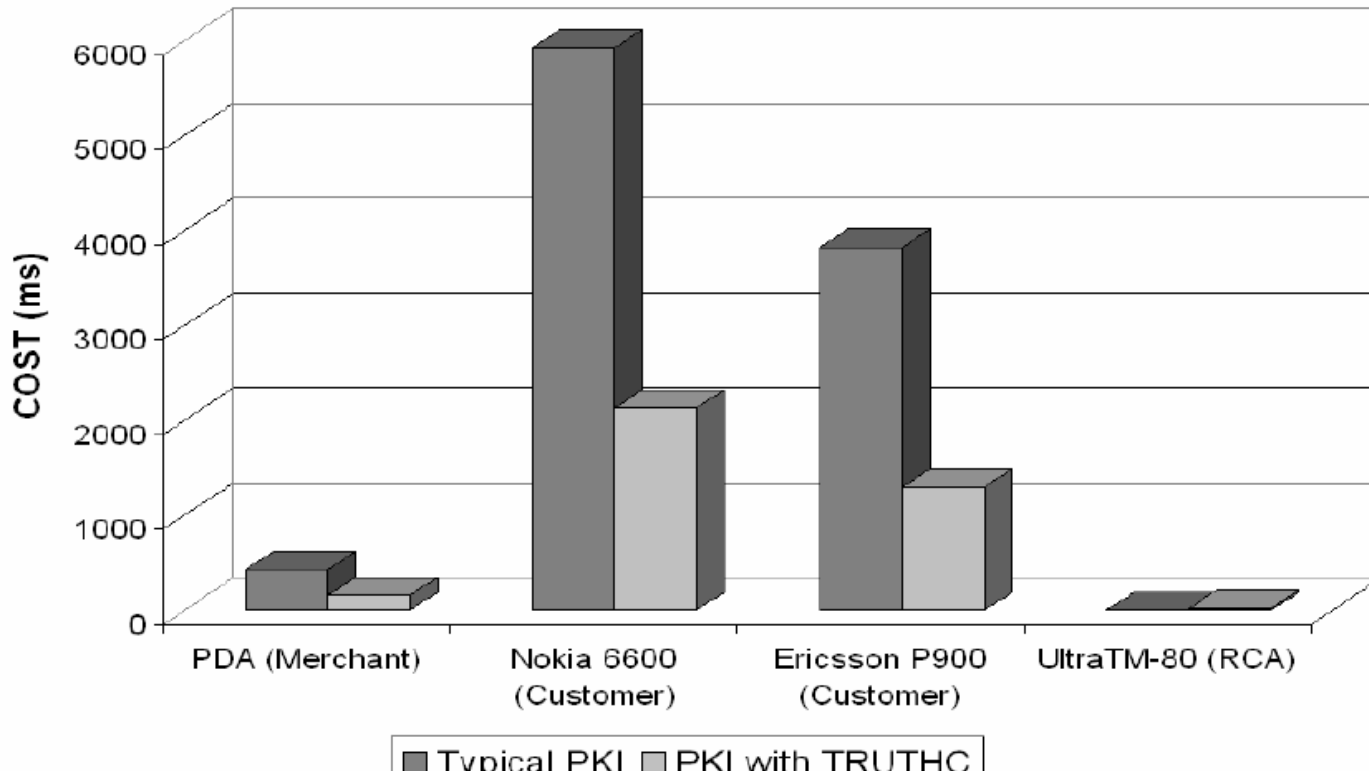
# EVALUATION

- **Computational cost using RSA-1937:  
Typical PKI vs. PKI with TRUTHC**



# EVALUATION

- **Computational cost using ECC-191:  
Typical PKI vs. PKI with TRUTHC**

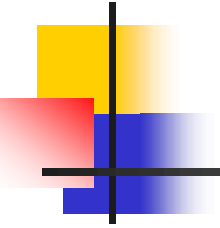




# CONCLUSIONS

---

- TRUTHC simplifies validation of cert paths for constrained devices
- TRUTHC is compatible with X.509 certificates
  - The integrity check value can be included as a certificate extension.
- TRUTHC reduces computational cost of mutual authentication in m-payment around 8% using RSA, and 60% using ECDSA.
- The m-payment scenario is just a sample scenario where TRUTHC may be used.



THANK YOU!!!