Blended Cryptography:

Public Key Infrastructure
for
Devices that don’t Public key

Phillip Hallam-Baker
Principal Scientist

VeriSign Inc.

Small is not beautiful

Not

When you write the code

PIC 16F88

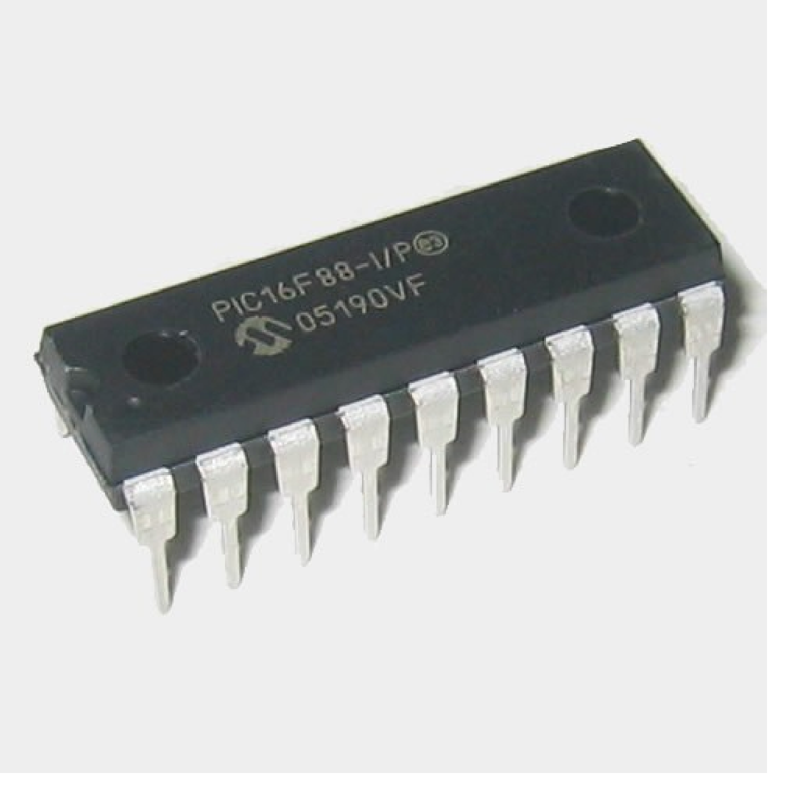
368 bytes RAM

4K Word ROM

20MHz

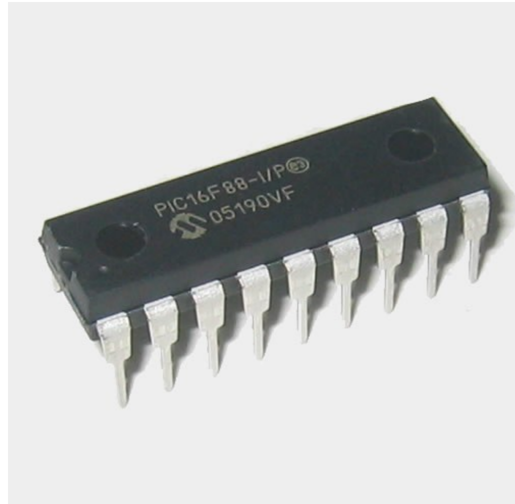
RS232/485 serial i/f

1kWh in 2,000 years




P R N D
220
240
260
CHECK TIRE PRESSURE
Auto : 000000
Inst Fuel : 000.0 l/100km

VeriSign®



<$1
(In quantity)

VeriSign®

The situation

- **Fact:** Can’t do Public Key
  - No, really, it can’t
- **Fact:** Can’t use bigger chip
  - Can’t grow out of the problem

- **Myth**: Cannot do PKI
  - Just have to do the PKI elsewhere

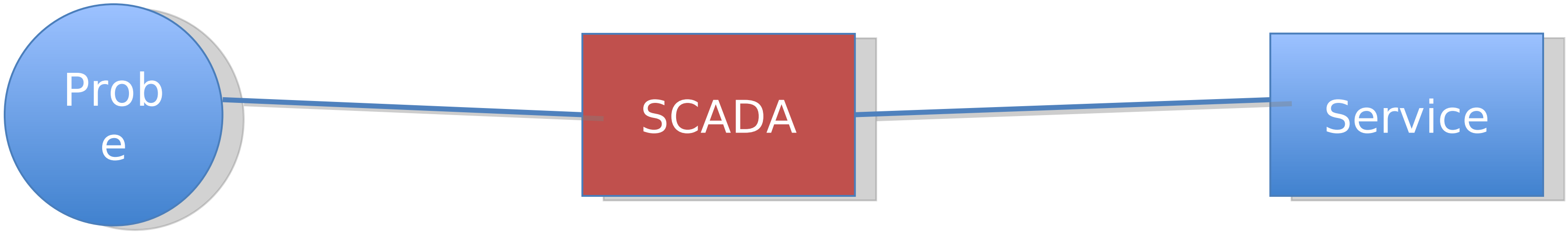
VeriSign®

Why PKI?

Automated Administration

SCADA

Delegated Key Agreement



Device ID

Master Secret

Certificate

Device ID

Master Secret

Shared

Shared

Nonces

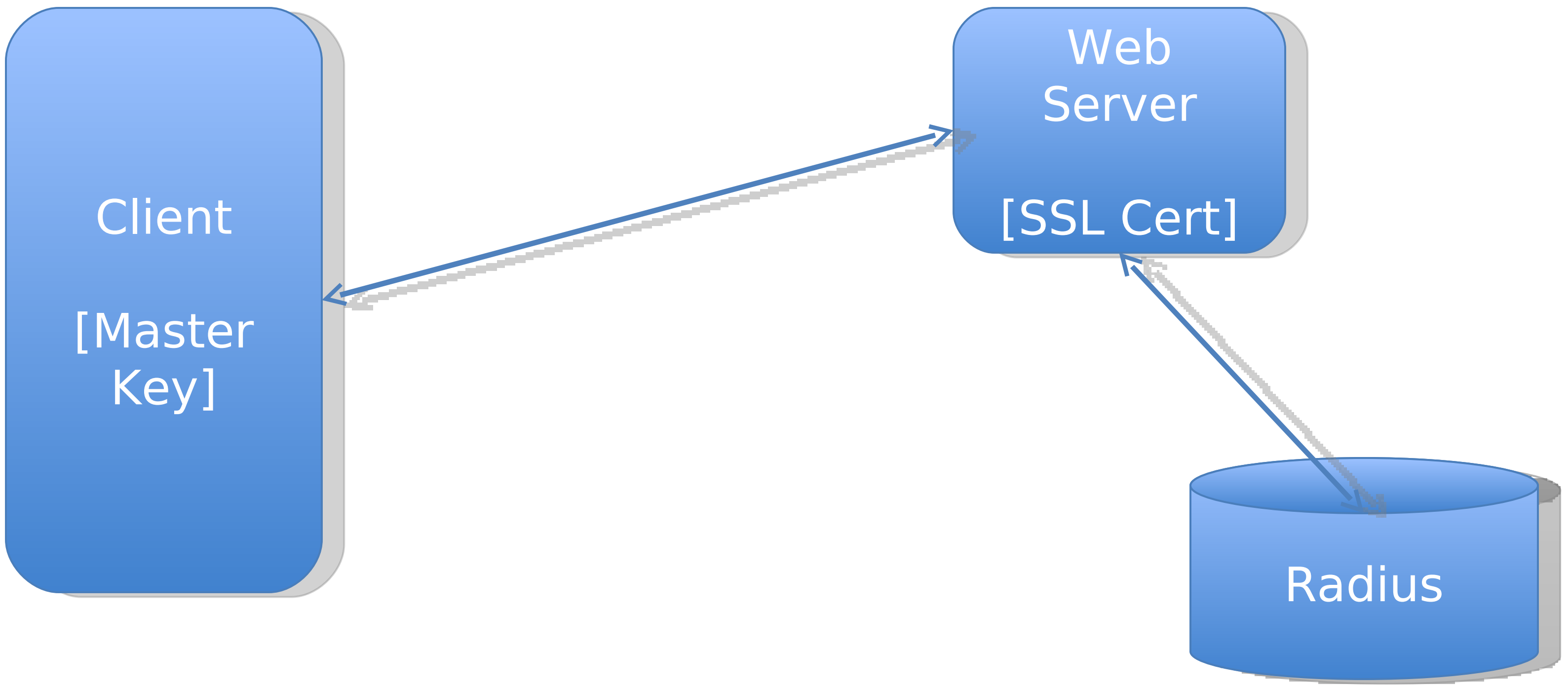
Mobile [User] Device

- Public Key Capable
- Limited Storage

Device Authentication
≠
User Authentication

VeriSign®

Transparent TLS Authentication



Shared Secret = MAC (ServerID, Master Key)
ServerID = H(Public Key) or
H(Issuer + Domain name) or
EV-ID

VeriSign®

Strong Authentication Credentials

- Implement TTLSA in microchip
  - Does not require public key

Traditional Approach

- Use public key to do all the interesting stuff
  - Use symmetric key for bulk crypto only
- Heavy number theory is impressively difficult
  - Get paper published at Crypto
  - No customer will ever accept it
- Wait for the symmetric key guys to

Blended Approach

Public Key Establishes Context

- If:
  - Party A knows the public key of Party B
- Or if:
  - Party A knows the public key of Party C that has a symmetric key relationship with party B

- Provides non-repudiation
  - (Whatever that might be)

Symmetric Key does ‘exotic’ effects

- Any random 128 value is a strong key
  - If k is a strong key then so is
    - H(k)
    - Mac (x, k)
    - Enc (x, k)
    - Enc (k, x)

Conclusions

- Every device that supports RS485
  - Can support strong cryptography
  - Can leverage PKI
    - Even if the device itself can't
- Blended Cryptography allows exotic effects
  - Without exotic public key

VeriSign®