RSA CONFERENCE 2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Applying Cryptography as a Service to Mobile Applications

SESSION ID: CSV-F02

Peter Robinson

Senior Engineering Manager
RSA, The Security Division of EMC

Introduction

- This presentation proposes a Cryptography as a Service (CaaS) model, which allows operations to be performed via web services.
- Core value proposition, without having keys on a mobile device:
  - Send and receive signed and encrypted messages.
  - View encrypted data stored on the phone.
  - View encrypted data stored in the cloud.

Objectives

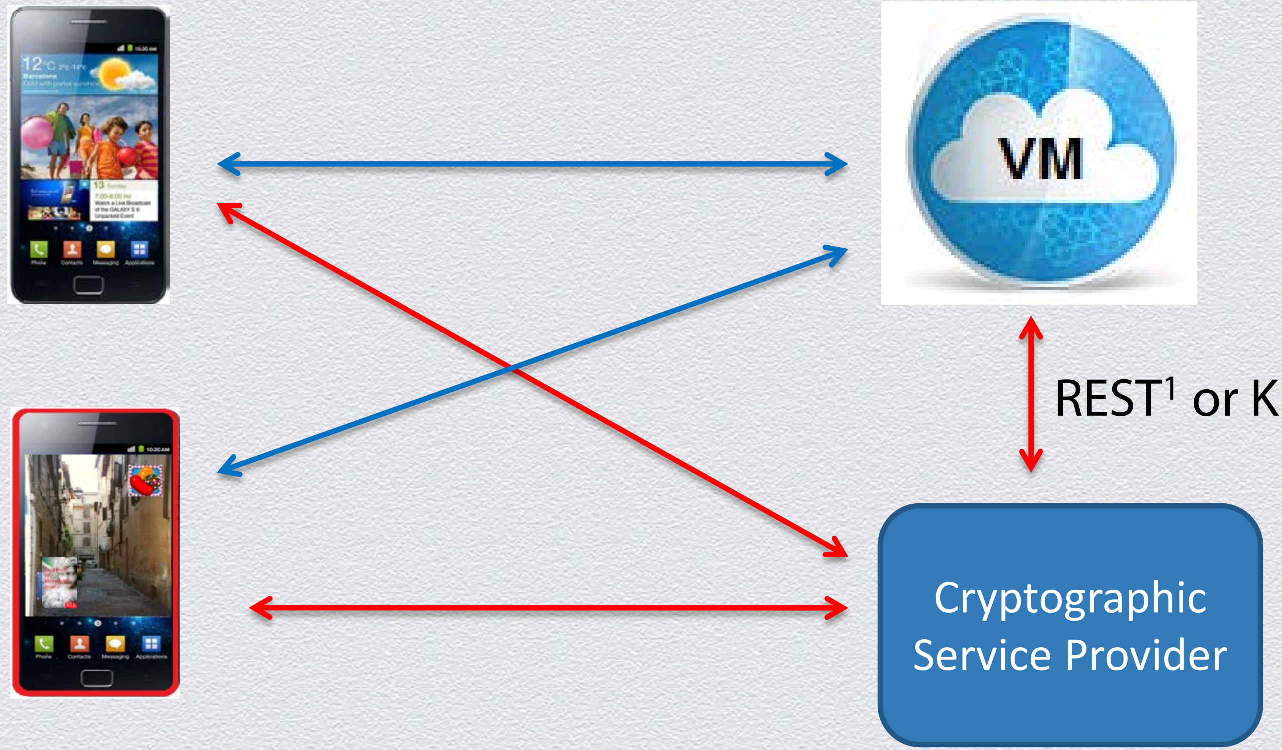
- As a result of this presentation you will be able to:
  - Define Cryptography as a Service (CaaS).
  - Describe the value proposition of CaaS.
  - Explain how to mitigate the challenges of CaaS.

CaaS Definition

CaaS Definition

- CaaS provides cryptographic operations on behalf of end points via web services.

CaaS Definition



REST[1] or KMIP[2]

Cryptographic Service Provider

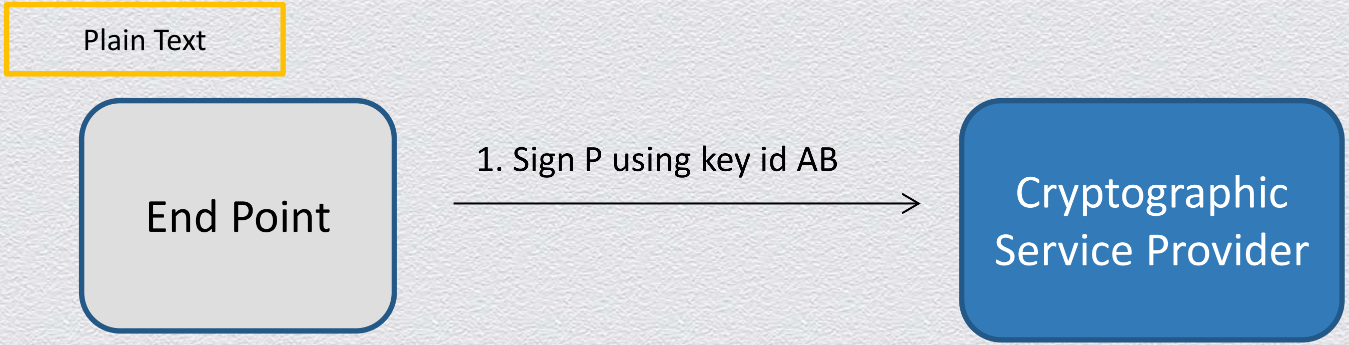
[1] Representational State Transfer over TLS.

[2] Key Management Interoperability Protocol over TLS.

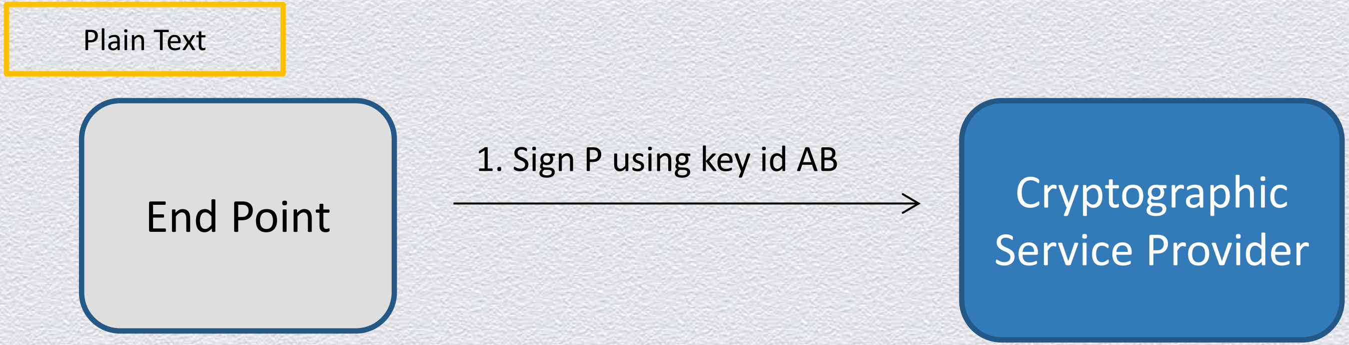
CaaS Definition

- Two core usages:
  - CaaS Providers can perform keyed cryptographic operations on behalf of end points via web services without exposing important cryptographic keys to the end points.
  - CaaS Providers can deliver entropy to end points to improve the quality of random numbers generated on the end points. This can be used to improve the quality of keys generated on the end points.

CaaS Definition: Keyed Operations



CaaS Definition: Keyed Operations



Plain Text

End Point

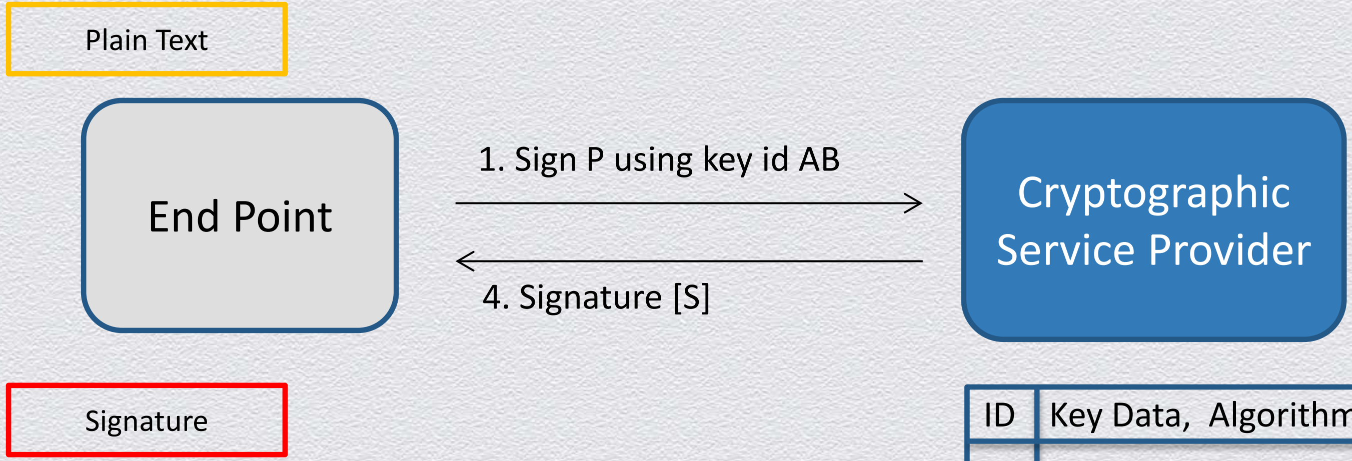
1. Sign P using key id AB

Cryptographic Service Provider

ID	Key Data, Algorithm, Key Type
AB	0x1234, ECDSA/SHA256, Private

2. Fetch key AB
3. S = Sign(ECDSA/SHA256, 0x1234, P)

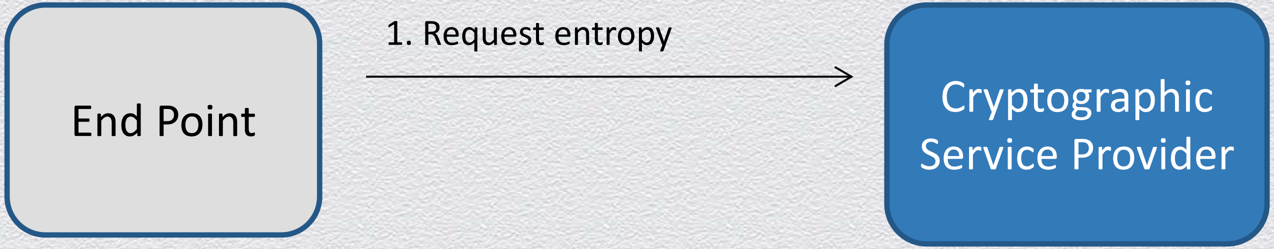
CaaS Definition: Keyed Operations



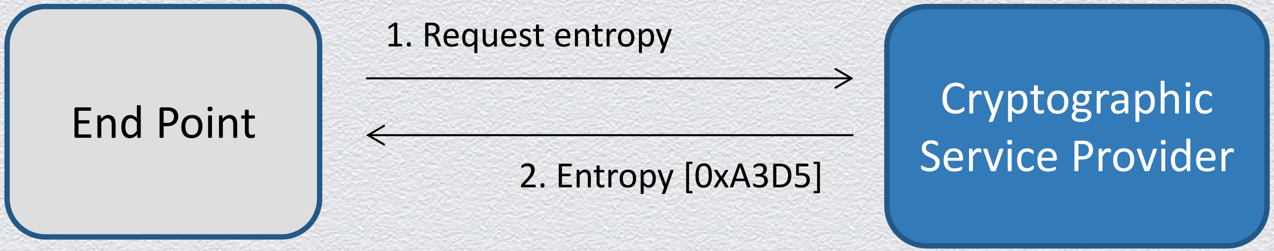
ID	Key Data,	Algorithm,	Key Type
AB	0x1234,	ECDSA/SHA256,	Private

2. Fetch key AB
3. S = Sign(ECDSA/SHA256, 0x1234, P)

CaaS Definition: Entropy Delivery Example



CaaS Definition: Entropy Delivery Example



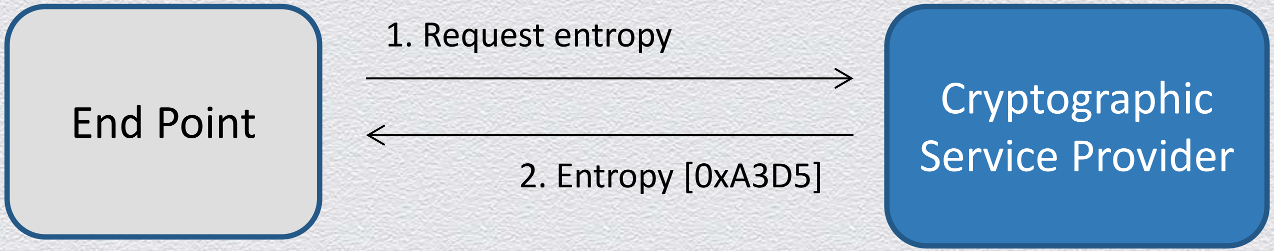
End Point

1. Request entropy

2. Entropy [0xA3D5]

Cryptographic Service Provider

CaaS Definition: Entropy Delivery Example



End Point

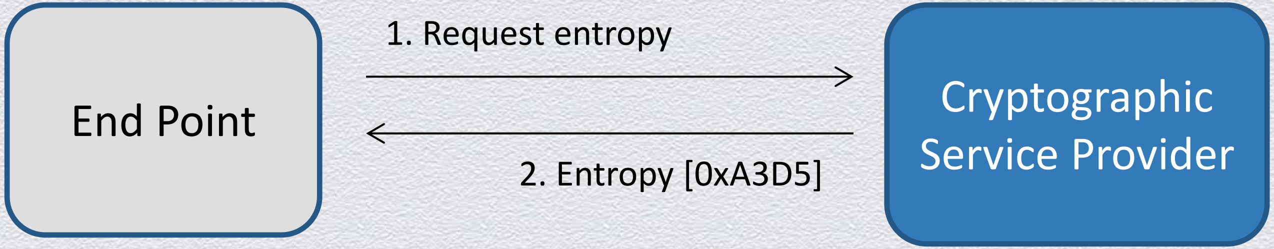
1. Request entropy

2. Entropy [0xA3D5]

Cryptographic Service Provider

3. PRNG mixes entropy [0xA3D5], updating its internal state.

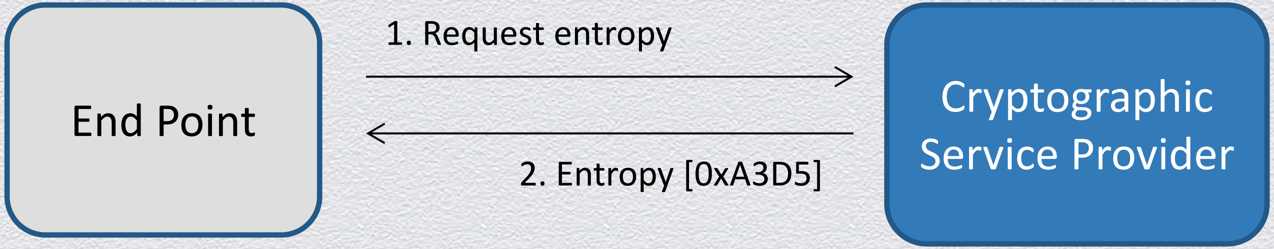
CaaS Definition: Entropy Delivery Example



3. PRNG mixes entropy [0xA3D5], updating its internal state.

NEVER
trust a single source of entropy.
CaaS entropy must be mixed with local entropy

CaaS Definition: Entropy Delivery Example



End Point

1. Request entropy

2. Entropy [0xA3D5]

Cryptographic Service Provider

3. PRNG mixes entropy [0xA3D5], updating its internal state.

4. Key generated based on random numbers produced by PRNG.

CaaS Questions: TLS and End Point Cryptography

- If a Transport Layer Security (TLS) connection can be established, then what is CaaS buying me?
  - Doesn’t TLS certificate path validation need to be done on the end point to verify that the end point is communicating with the CaaS Provider?
    - The TLS certificate path validation uses *public* keys.
    - CaaS aims to prevent exposure of important *private* keys at the end point.
  - Client authentication:
    - Not reliant on TLS Client Certificates and *private* keys.
    - Advanced multi-factor authentication methods are required.

CaaS Questions: Comparison of HSM and CaaS[1]

CaaS	Hardware Security Module (HSM)
Scalability and on demand elastic scaling	Fixed scaling
Virtual Machine	Hardware
Higher Performance	Lower Performance
Wider API support / more flexible APIs KMIP, REST / Proprietary, (and PKCS #11)	Narrower API support / less flexible APIs PKCS #11, Proprietary, (and KMIP)
FIPS 140 Security Level 1 or 2	FIPS 140 Security Level 3 or 4
Lower cost	Higher cost

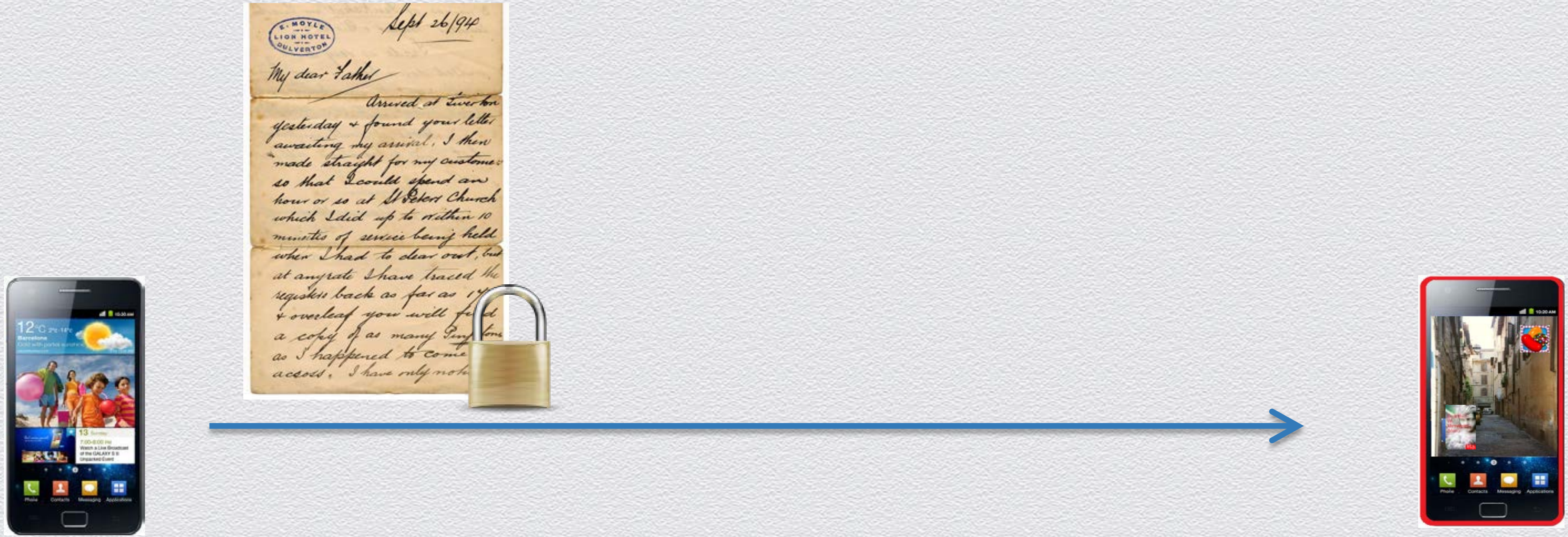
1. This table contains generalizations which may not be true for all vendors.

CaaS Value Proposition

Value Proposition

- Without having keys on the phone, CaaS allows:
  - Sending and receiving signed and encrypted messages.
  - Viewing encrypted data stored on the phone.
  - Viewing encrypted data stored in the cloud.
- Simple credential sharing.
- Centralized management.
- Improved security.

Value Proposition: Signed and Encrypted Messages



E. MOYLE
LION HOTEL
DULVERTON

Sept 26/94

My dear Father

Arrived at Tiverton yesterday + found your letter awaiting my arrival. I then made straight for my customers so that I could spend an hour or so at St Peters Church which I did up to within 10 minutes of service being held when I had to clear out, but at anyrate I have traced the registers back as far as 17 + overleaf you will find a copy of as many Pimftons as I happened to come across. I have only noh

Alice

Bob

Value Proposition: Signed and Encrypted Messages

Alice

Cryptographic Service Provider

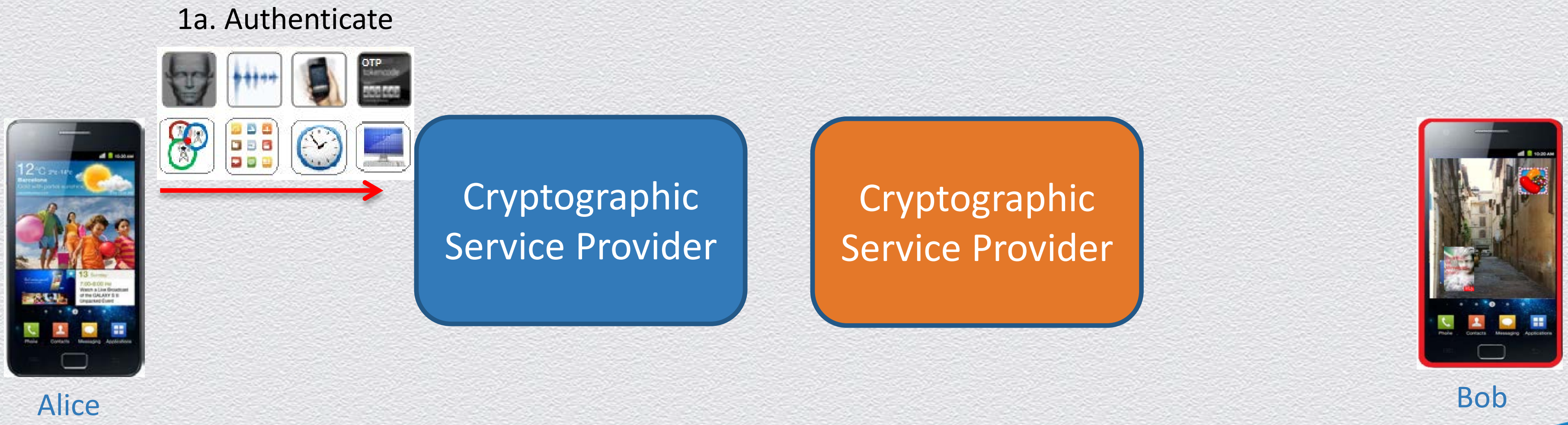
Alice registered.
Alice's Private Keys
Bob's Public Keys

Cryptographic Service Provider

Bob registered.
Alice's Public Keys
Bob's Private Keys

Bob

Value Proposition: Signed and Encrypted Messages



1a. Authenticate

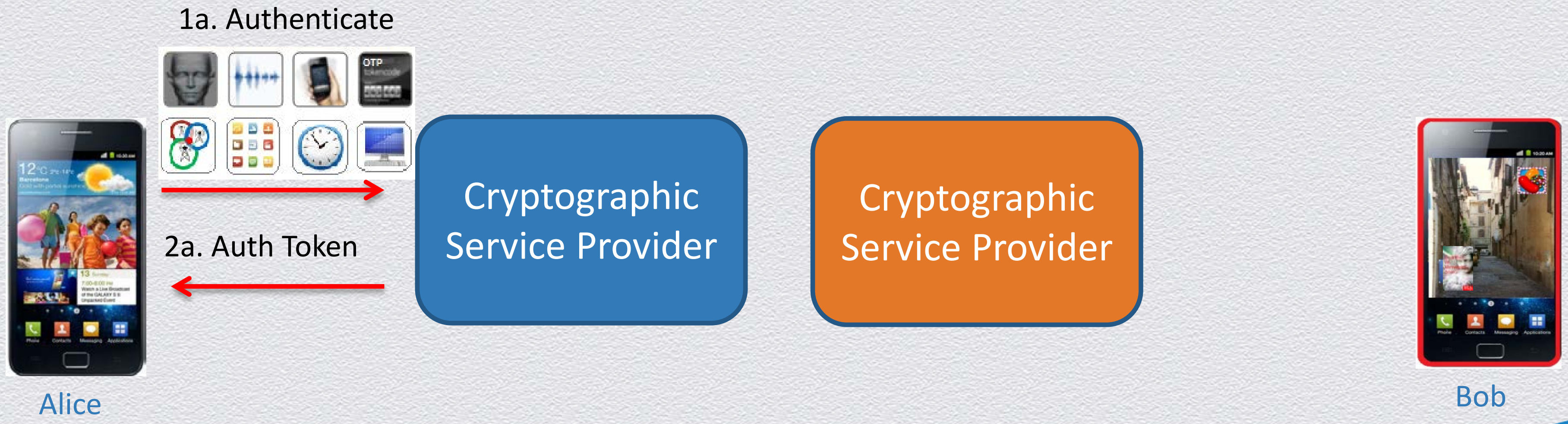
Cryptographic Service Provider

Cryptographic Service Provider

Alice

Bob

Value Proposition: Signed and Encrypted Messages



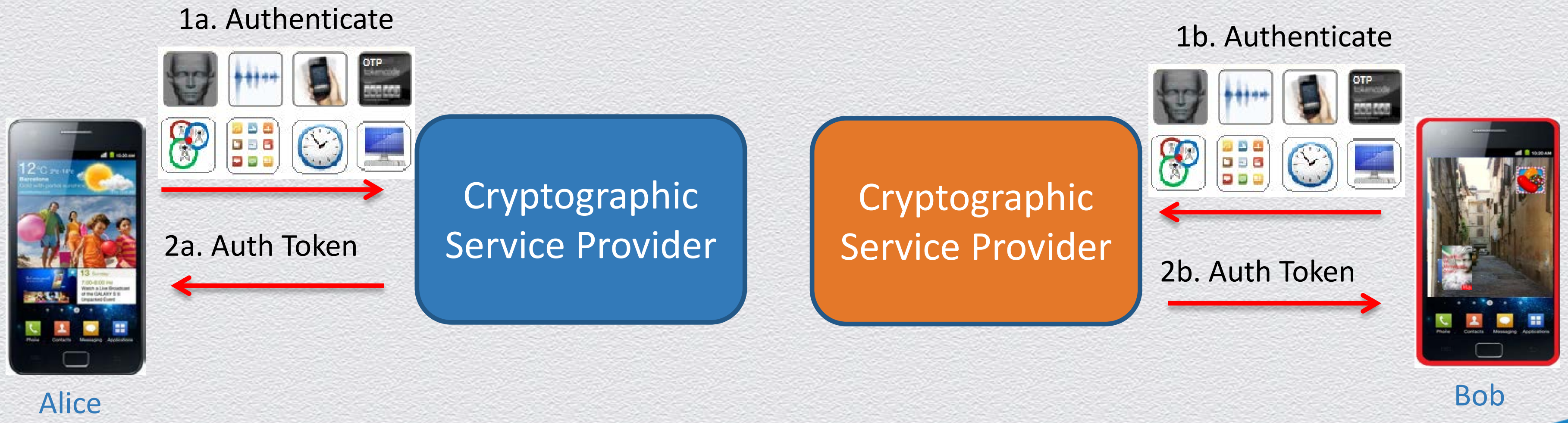
1a. Authenticate

2a. Auth Token

Cryptographic Service Provider

Cryptographic Service Provider

Value Proposition: Signed and Encrypted Messages



1a. Authenticate

2a. Auth Token

Cryptographic Service Provider

Cryptographic Service Provider

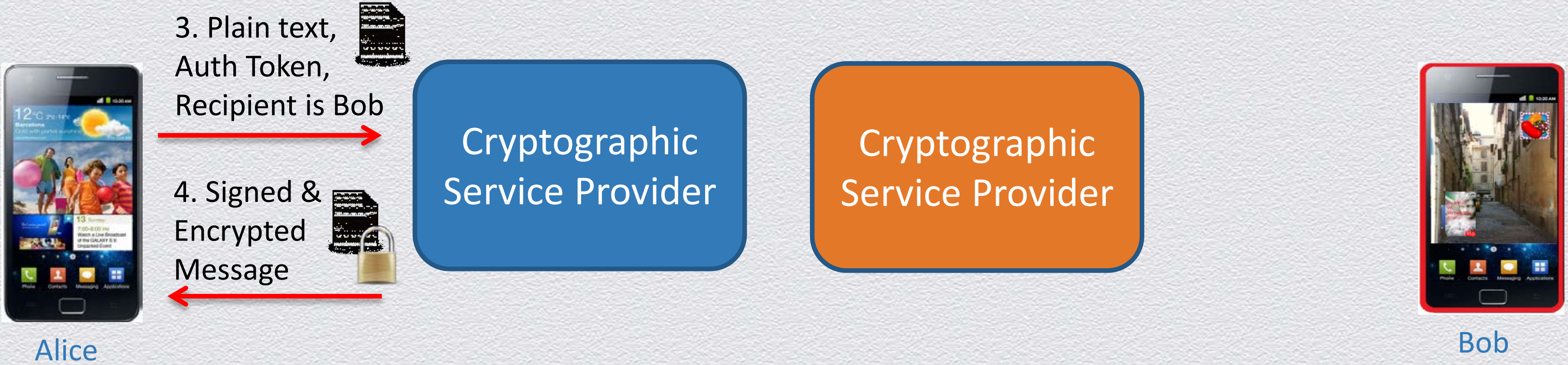
1b. Authenticate

2b. Auth Token

Alice

Bob

Value Proposition: Signed and Encrypted Messages



3. Plain text, Auth Token, Recipient is Bob

4. Signed & Encrypted Message

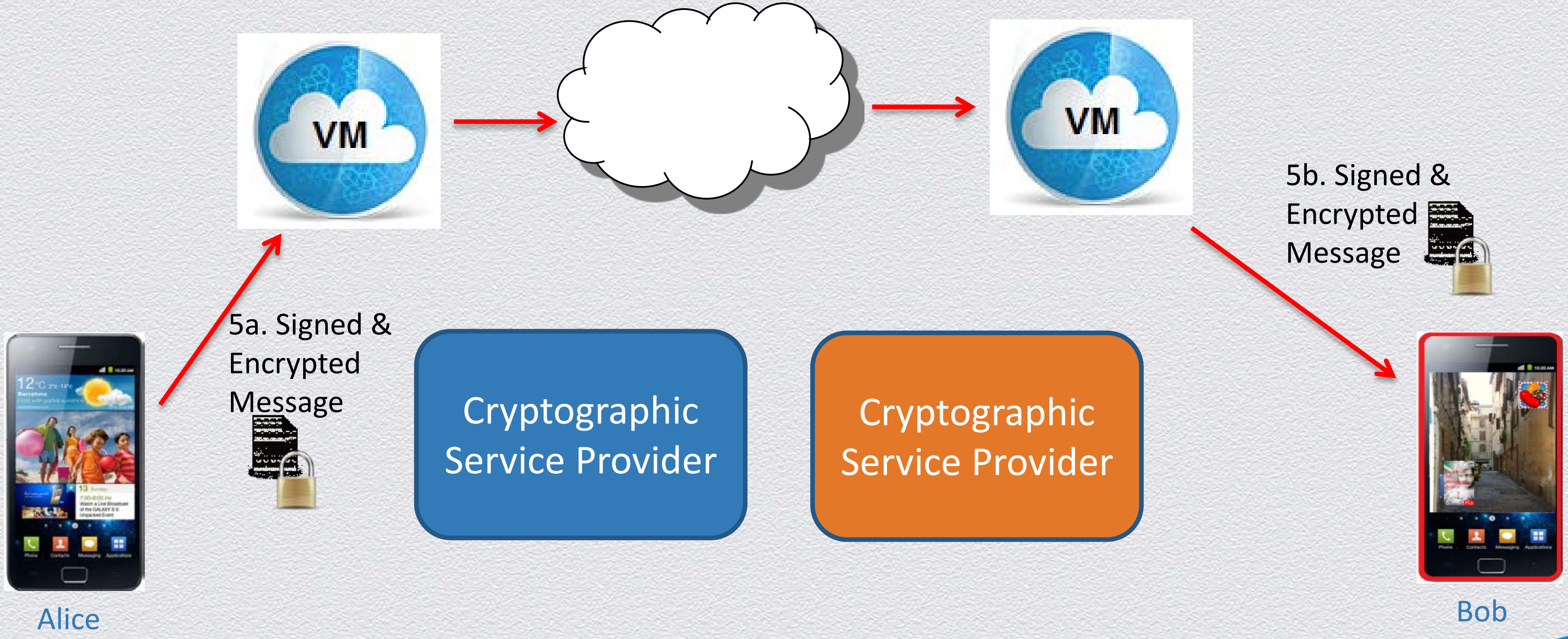
Cryptographic Service Provider

Cryptographic Service Provider

Alice

Bob

Value Proposition: Signed and Encrypted Messages



VM

VM

5a. Signed & Encrypted Message

5b. Signed & Encrypted Message

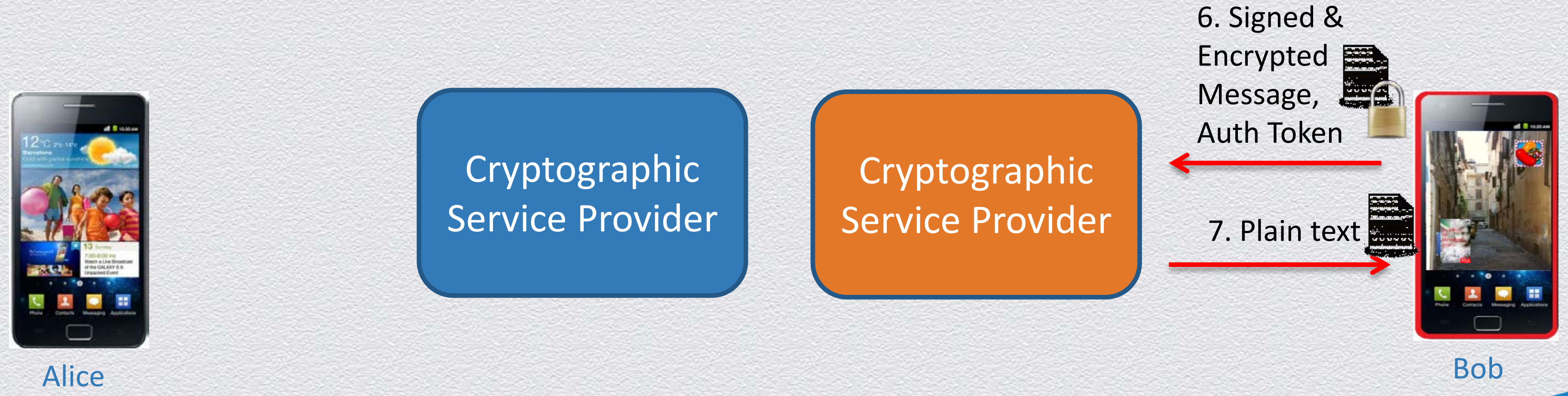
Cryptographic Service Provider

Cryptographic Service Provider

Alice

Bob

Value Proposition: Signed and Encrypted Messages



Cryptographic Service Provider

Cryptographic Service Provider

6. Signed & Encrypted Message, Auth Token

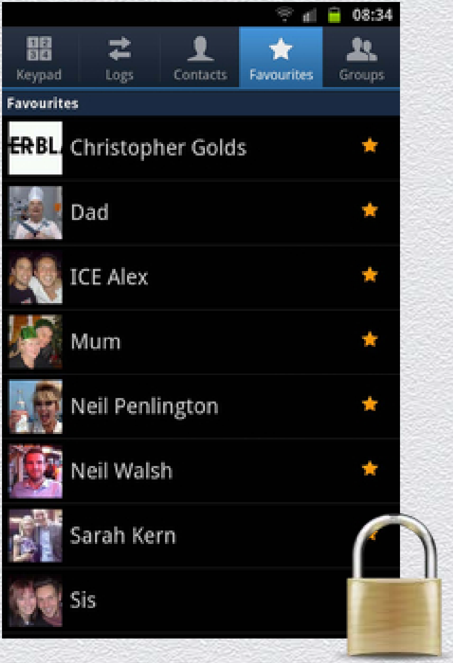
7. Plain text

Alice

Bob

Value Proposition: Encrypted Local Data

Alice



Favourites

- Christopher Golds
- Dad
- ICE Alex
- Mum
- Neil Penlington
- Neil Walsh
- Sarah Kern
- Sis

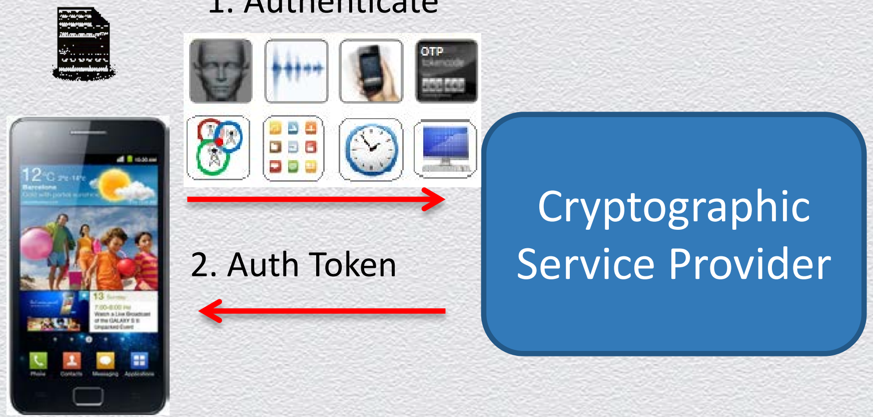
Value Proposition: Encrypted Local Data

Alice

Cryptographic Service Provider

Alice registered.
Alice's Secret Key

Value Proposition: Encrypted Local Data



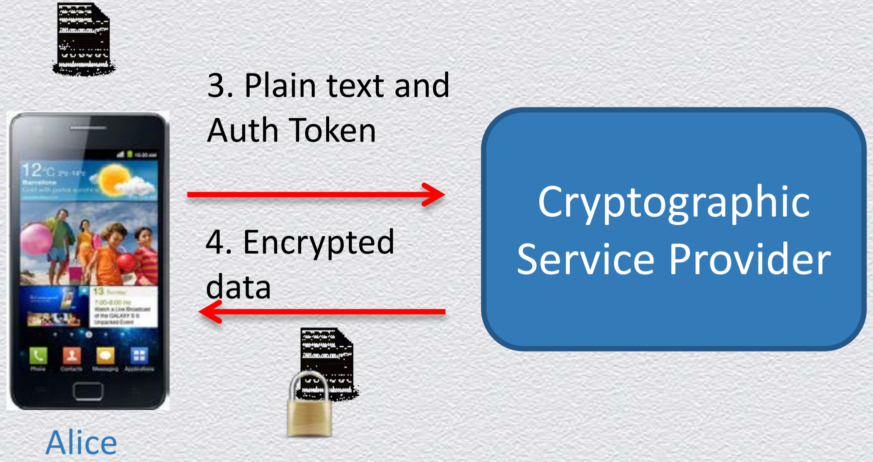
1. Authenticate

2. Auth Token

Cryptographic Service Provider

Alice

Value Proposition: Encrypted Local Data



Alice

3. Plain text and Auth Token

4. Encrypted data

Cryptographic Service Provider

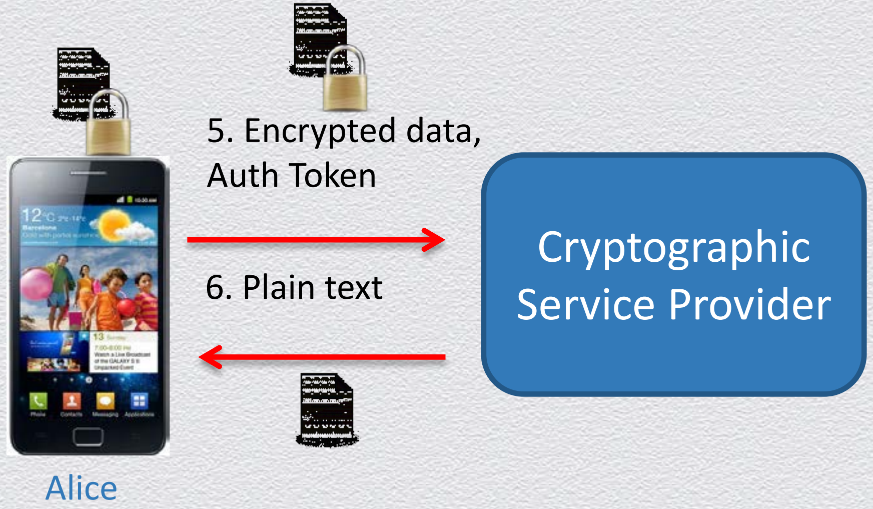
Value Proposition: Encrypted Local Data

Alice

Cryptographic Service Provider

Alice registered.
Alice’s Secret Key

Value Proposition: Encrypted Local Data



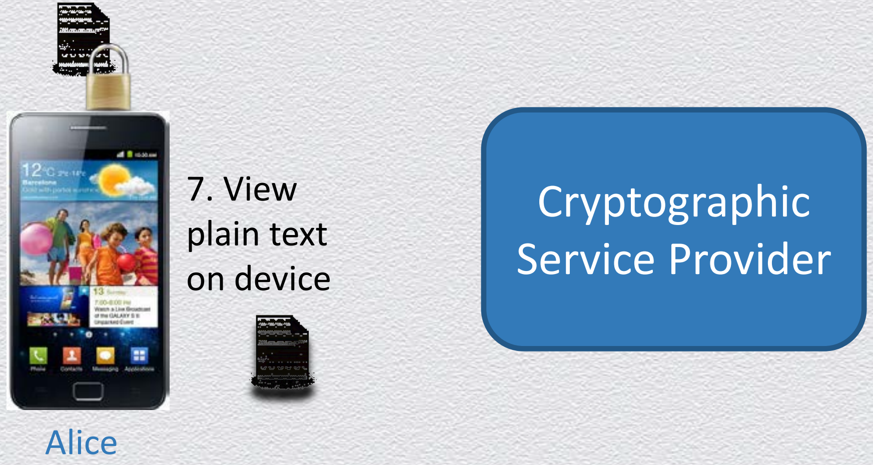
5. Encrypted data, Auth Token

6. Plain text

Cryptographic Service Provider

Alice

Value Proposition: Encrypted Local Data

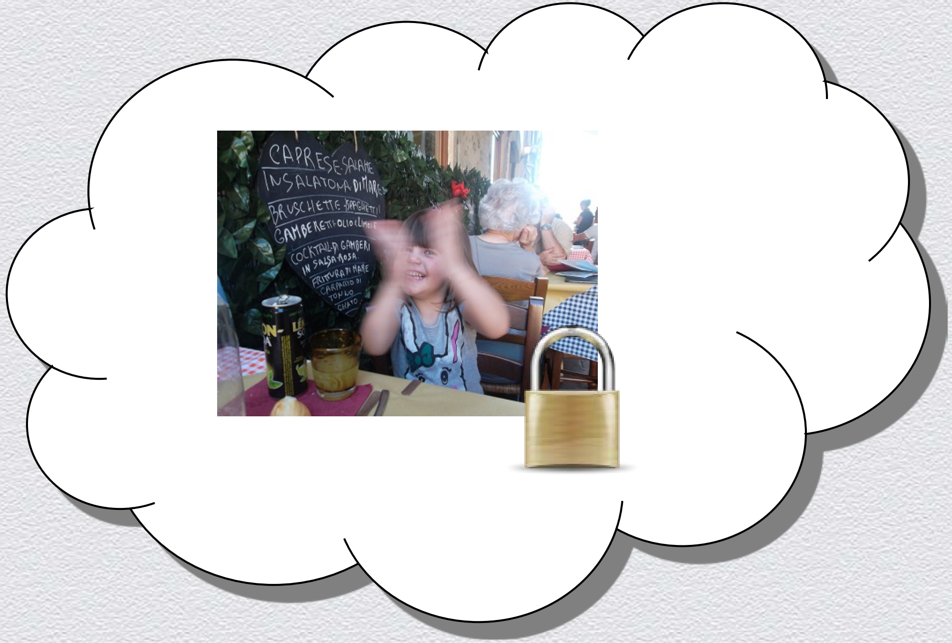


7. View plain text on device

Cryptographic Service Provider

Alice

Value Proposition: Encrypted Cloud Data



Alice

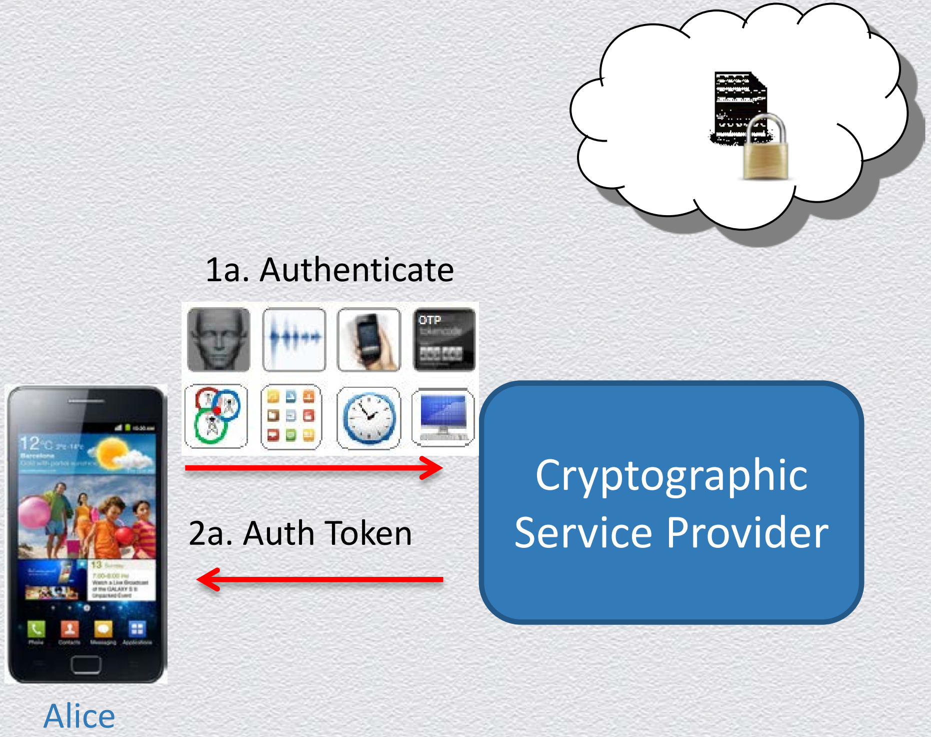
Value Proposition: Encrypted Cloud Data

Alice

Cryptographic Service Provider

Alice registered.
Secret Key which
Alice has access to.

Value Proposition: Encrypted Cloud Data



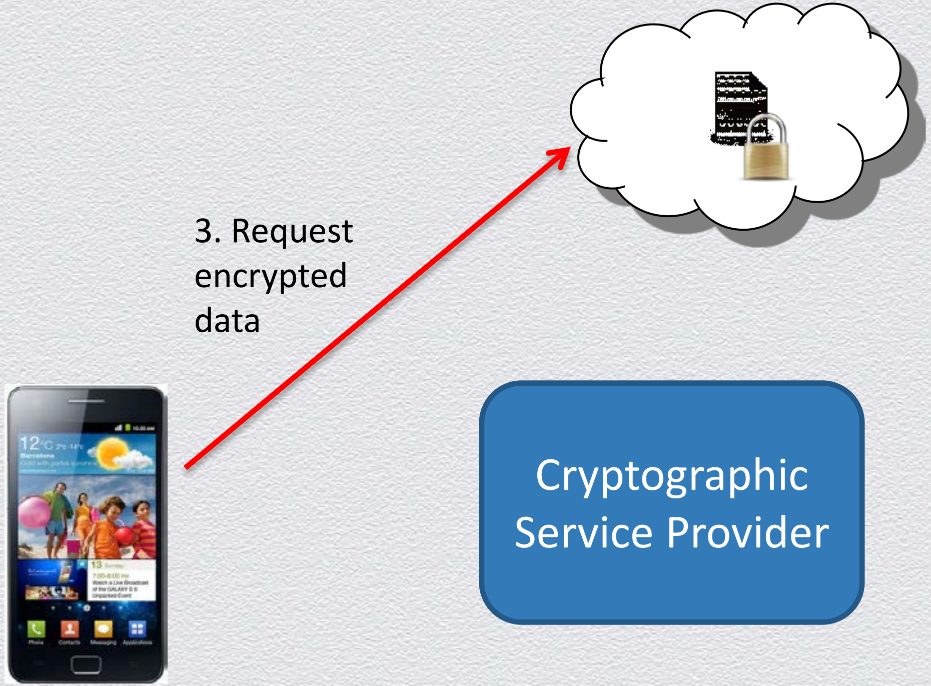
1a. Authenticate

2a. Auth Token

Cryptographic Service Provider

Alice

Value Proposition: Encrypted Cloud Data

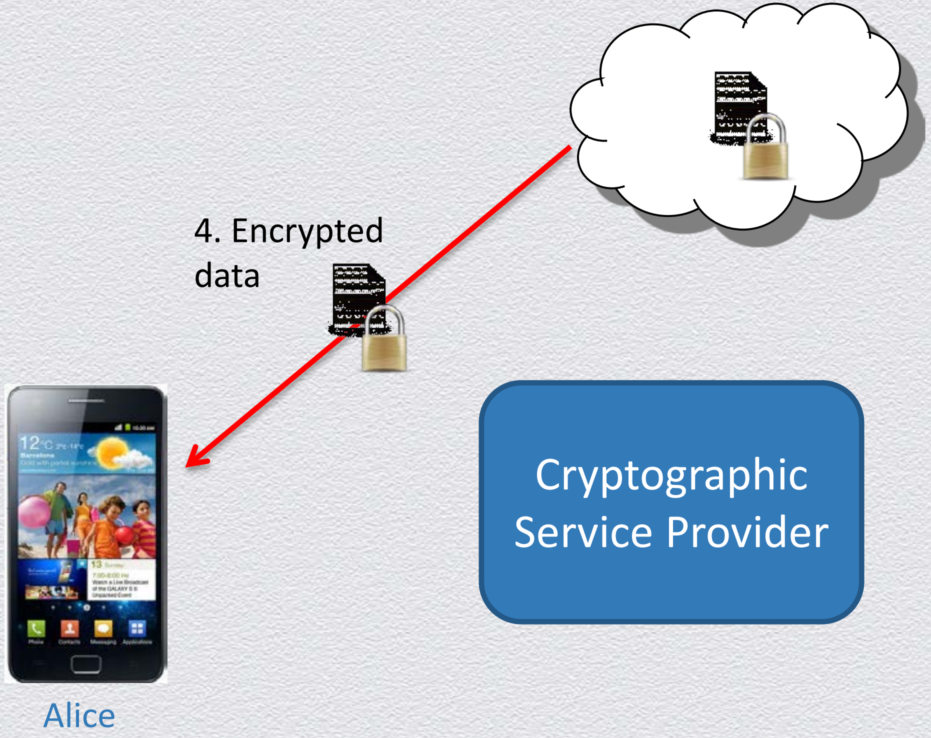


3. Request encrypted data

Cryptographic Service Provider

Alice

Value Proposition: Encrypted Cloud Data

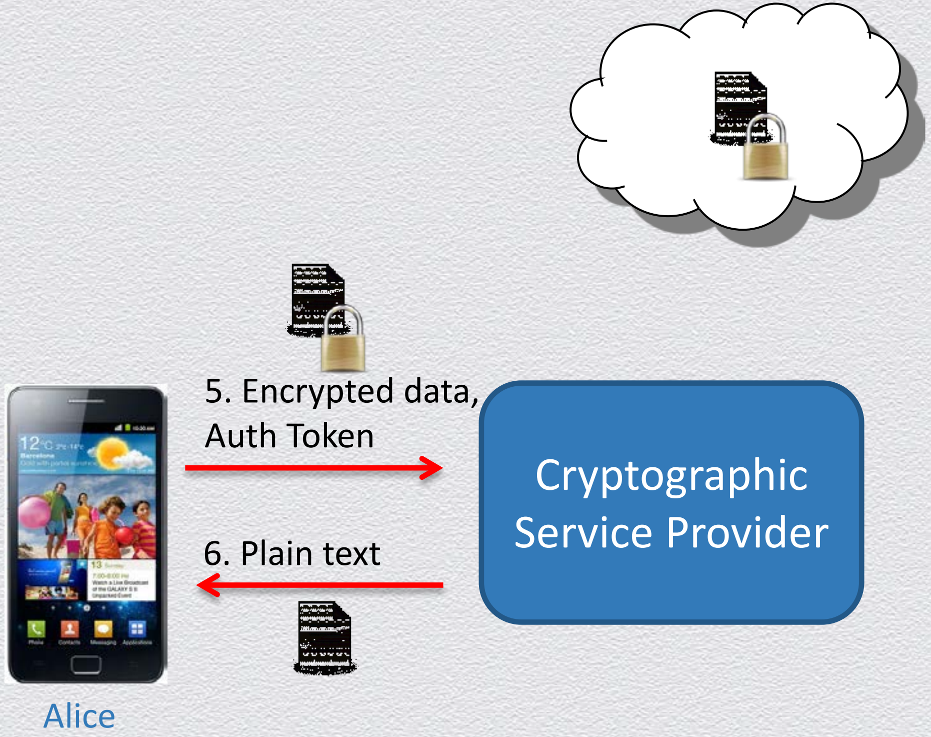


4. Encrypted data

Cryptographic Service Provider

Alice

Value Proposition: Encrypted Cloud Data



5. Encrypted data, Auth Token

6. Plain text

Cryptographic Service Provider

Alice

Value Proposition: Credential Sharing

- Credential sharing between mobile devices.

Value Proposition: Centralized Management

- Important keys reside in the CaaS provider.
  - Back-up and restore easier.
  - Could allow keys and certificates to be automatically rolled-over.
  - Game theory and technologies such as FlipIT[1] can be used to improve the security of keys.

[1] For details see: https://blogs.rsa.com/applying-game-theory-to-cybersecurity-game-theory-at-rsa-conference-europe-2012/

Value Proposition: Improved Security

- Improved security if keys reside in CaaS provider:
  - No important cryptographic keys on end points.
  - Important cryptographic keys stored and backed up in one place.
- Improved security if entropy is delivered:
  - Keys which are generated on the end point have improved quality.

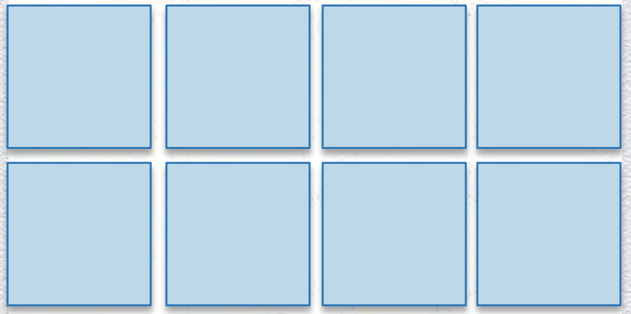
CaaS Challenges

CaaS Challenges: End Point Authentication

- End Point Authentication ensures only authorized end points can use the CaaS services.

CaaS Challenges: End Point Authentication

- User:
  - Password.
  - Voice print.
  - Facial recognition.
  - Motion based.
  - One Time Password.



CaaS Challenges: End Point Authentication

- Environment:
  - Device: Device ID, SIM number, Phone number, MAC Address.
  - Location.
  - Apps allowed to be on phone.
  - Time of day.

CaaS Challenges: End Point Authentication

- Risk based authentication could be applicable:
  - Services available depend on the degree to which the identity is authenticated.
  - Alternatively, the level of authentication could be “stepped-up” if the requested service requires a higher degree of authentication than has been provided.

CaaS Challenges: Server Authentication

- End points must trust the Cryptographic Service Provider.
- Typically achieved by TLS Server Authentication.
- If an attacker can fool the end point into trusting another Cryptographic Service Provider, then the end point is probably fully compromised (Powerfully Owned).

CaaS Challenges: CaaS Provider Security

- CaaS Provider as an attack target:
  - Contains a cache of important keys.
  - User authentication information.
- Mitigations:
  - Need to prevent memory snap shots of the CaaS Provider VMs.
  - Encrypt back-ups.
  - Locate in a private cloud.

CaaS Challenges: Network Connectivity

- Mobile devices need to have network connectivity to CaaS provider.
  - Perhaps this is not a challenge.
  - If a mobile device can not connect to the CaaS provider, should it be able to do operations which require sensitive keys?

Closing

How to Apply this Knowledge

- Review what end points you have.
- For each end point:
  - Which keys are on the end point?
  - Is the entropy on end points sufficient to generate keys?
  - What cryptographic operations are performed and why?
  - What would be the cost of key compromise?
  - Which cryptographic operations would be suitable for a CaaS model?
  - What authentication mechanisms could be used?

Summary

- CaaS provides cryptographic operations on behalf of end points via web services.
    - Keyed crypto services without exposing important keys to end points.
    - Entropy delivery to end points to improve key generation quality.
- CaaS combined with strong authentication solves security conundrums:
    - Using secure messaging credentials with mobile devices.
    - Using encrypted data stored on a mobile device.
    - Viewing encrypted cloud data on mobile devices.

Questions

Peter Robinson

peter.robinson@rsa.com