



KEYPROV

Phillip Hallam-Baker – Principal Scientist: pbaker@verisign.com

September 24th 2008



What's in the box

- + 1 Protocol
 - Dynamic Symmetric Key Provisioning Protocol
- + 2 Key Container Formats
 - Portable Symmetric Key Container
 - Symmetric Key Package Content Type

DRAFT



An IETF Working Group

- + Scope excludes work by other working groups
 - NOT Key Exchange (IPSEC, TLS)
 - NOT Public Key Infrastructure (PKIX, PGP)
 - NOT Long Term Archiving (LTRANS)
 - NOT Key Release based DRM

- + So what is left?

DRAFT



Starting Problem

+ One Time Password Token Provisioning

DRAFT



General case of

- + Initial Establishment of Symmetric Key

- + Applications
 - Wireless provisioning of OTP device
 - Provisioning of keys to Hardware encryption device
 - Provisioning of keys to embedded device

Necessary sub-problem

- + Management of Symmetric Key Credential
- + Requires
 - Syntax for Symmetric Key Container

Mapping to Public Key Infrastructure

- + Protocol = PKCS #10
- + Key Container = PKCS# 12

DRAFT



KEYPROV Symmetric Key Containers

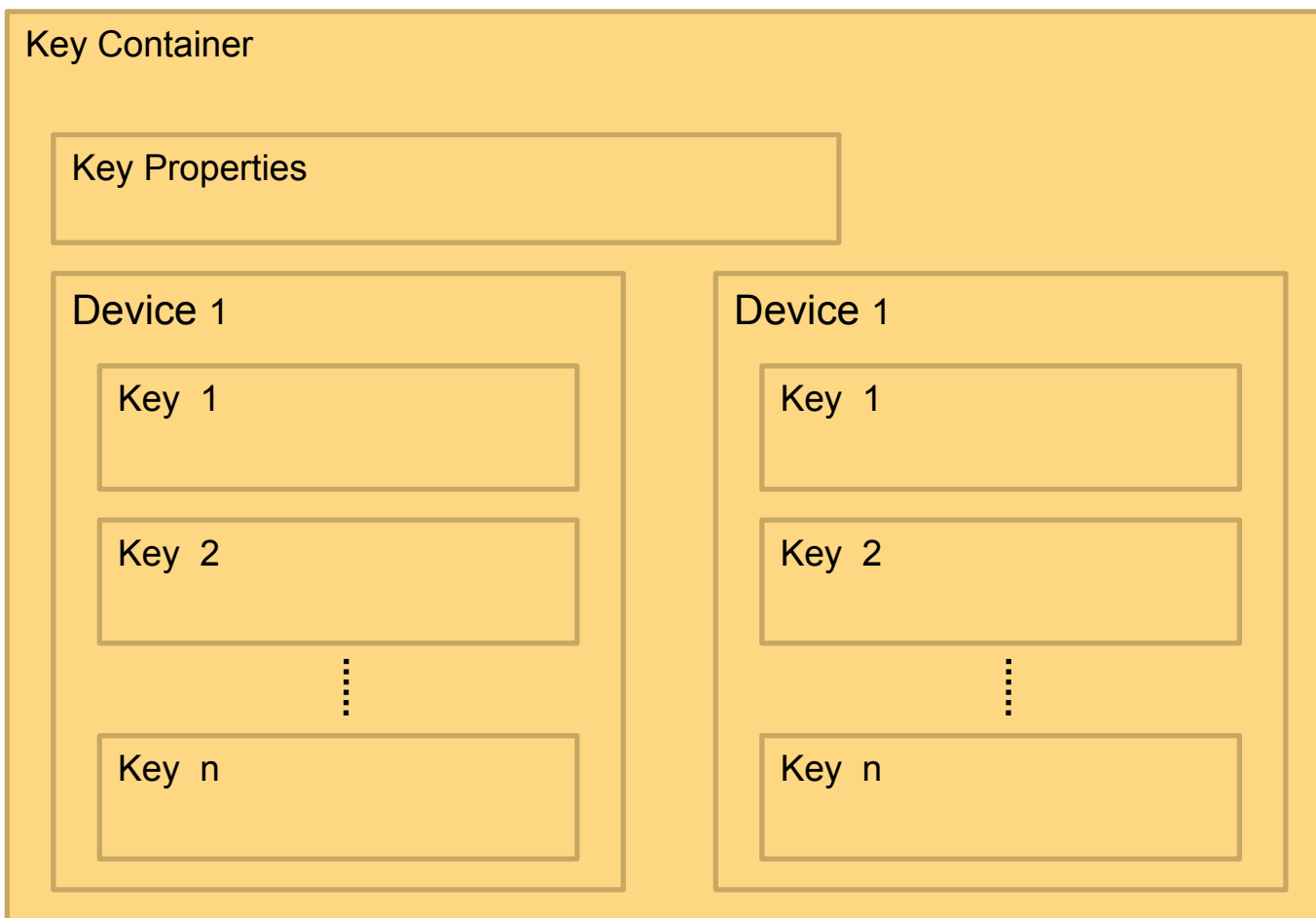
- + Portable Symmetric Key Container (PSKC)
 - XML Syntax

- + Symmetric Key Package
 - ASN.1 alternative to PSKC
 - ASN.1 is the XML of cryptography
 - Crypto Modules MUST support ASN.1
 - Do not want to create requirement for validated XML handler

DRAFT



Inside PSKC



DRAFT



DSKPP – The Protocol

- + Single or multiple key requests
- + Optional User Authentication
 - By means of out of band issued pass code
- + Time Out Policy
- + Key Renewal
 - Including replacement of pre-loaded key
- + Pre-shared Manufacturing key
- + End-to-End Protection of keying material

DRAFT



4-Pass or 2-pass protocol

+ Use 4-Pass if

- Both parties are required to contribute entropy to the established key
- Cryptomodule does not have private key capability
- Cryptomodule does not have pre-issued key or keypad capability

+ Use 2-Pass if

- Must provision pre-existing key
- Have either pre-issued key or a built-in keypad.

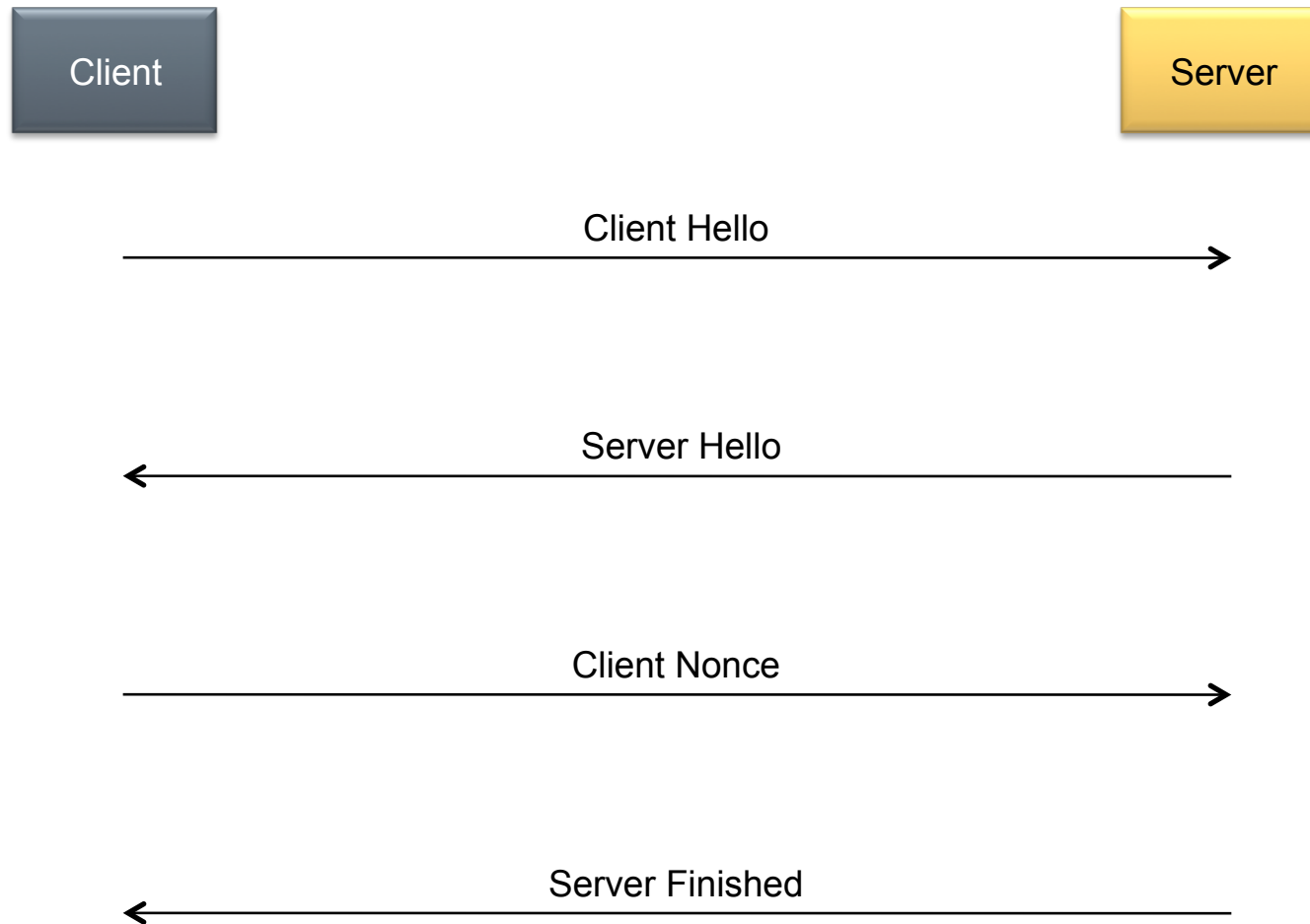
Trigger Message

- + DSKPP is initiated by client
 - Server may request client initiate request
 - Trigger message contains R_TRIGGER identifier

DRAFT



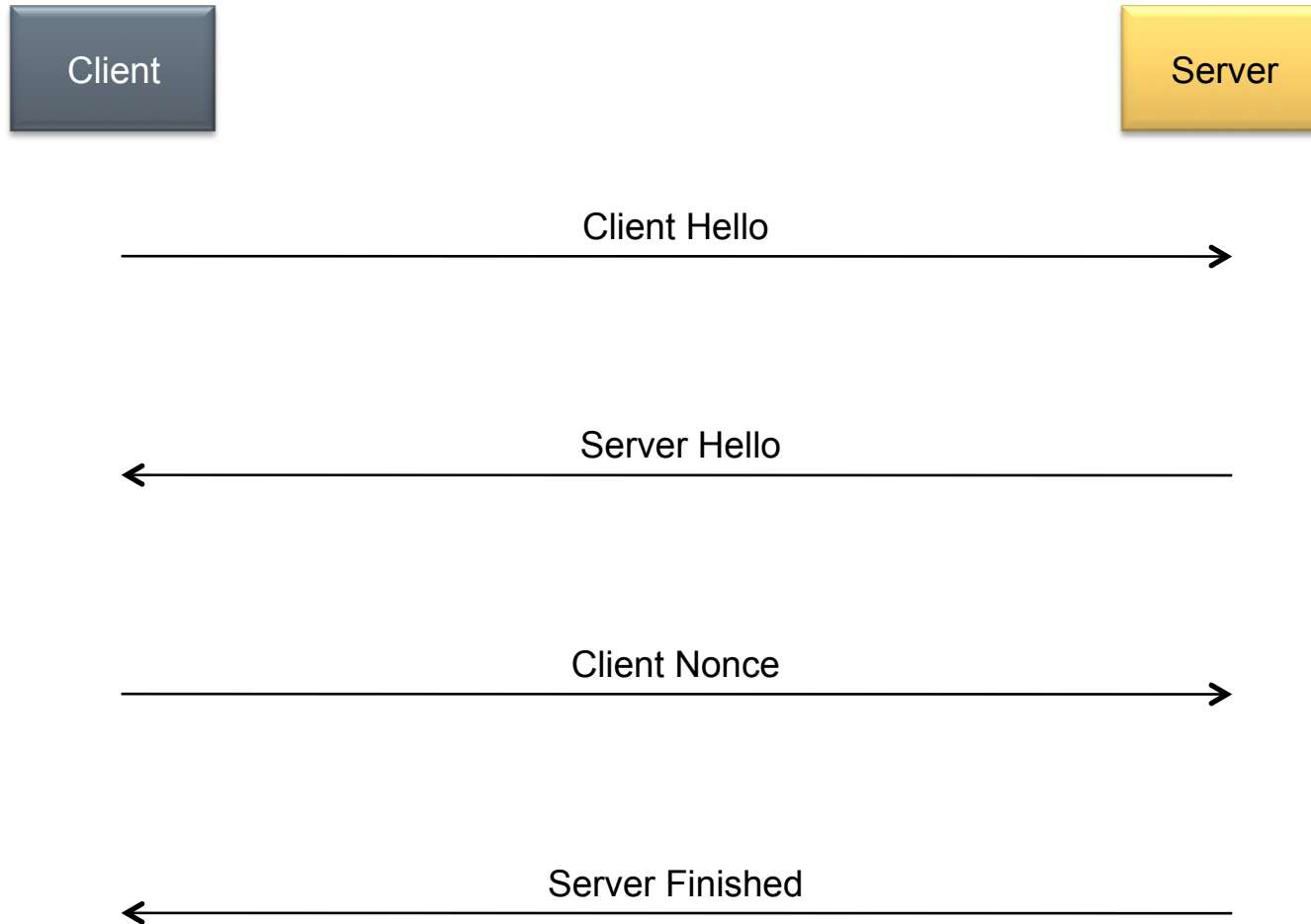
Protocol Transactions – 4 Pass



DRAFT



Protocol Transactions – 2 Pass



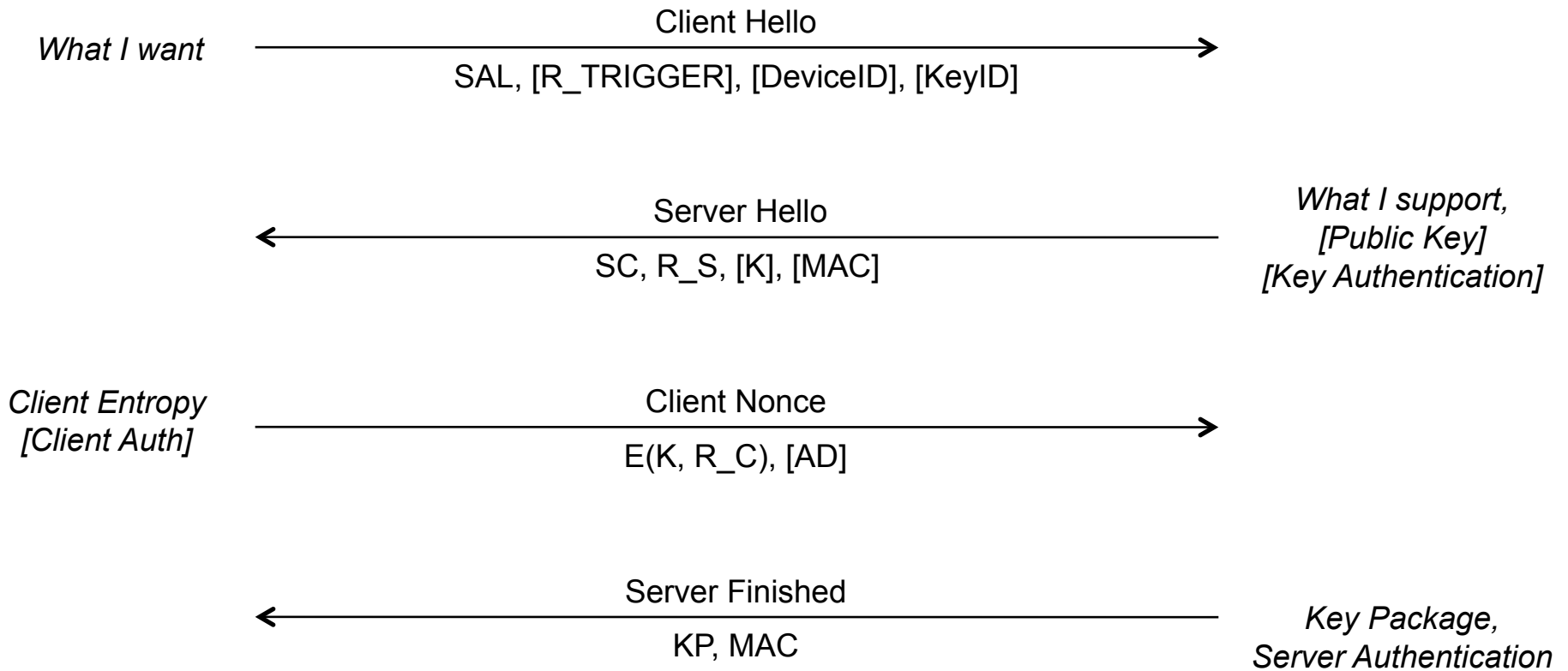
DRAFT



Protocol Transactions – 4 Pass

Client

Server



DRAFT



Why is authentication 'optional'?

- + May be delivered by hardware context
 - e.g hardware module plugged in to USB port
- + May be delivered by lower protocol layer
 - e.g layer over HTTPS

Conclusion

- + KEYPROV provides
 - Protocol for initial key establishment
 - Symmetric key container formats for ASN.1, XML
- + KEYPROV does not provide
 - Generic key exchange (see WS-*, IPSEC, TLS)
 - Asymmetric key handling (see XKMS, PKIX)



Thank You!

