

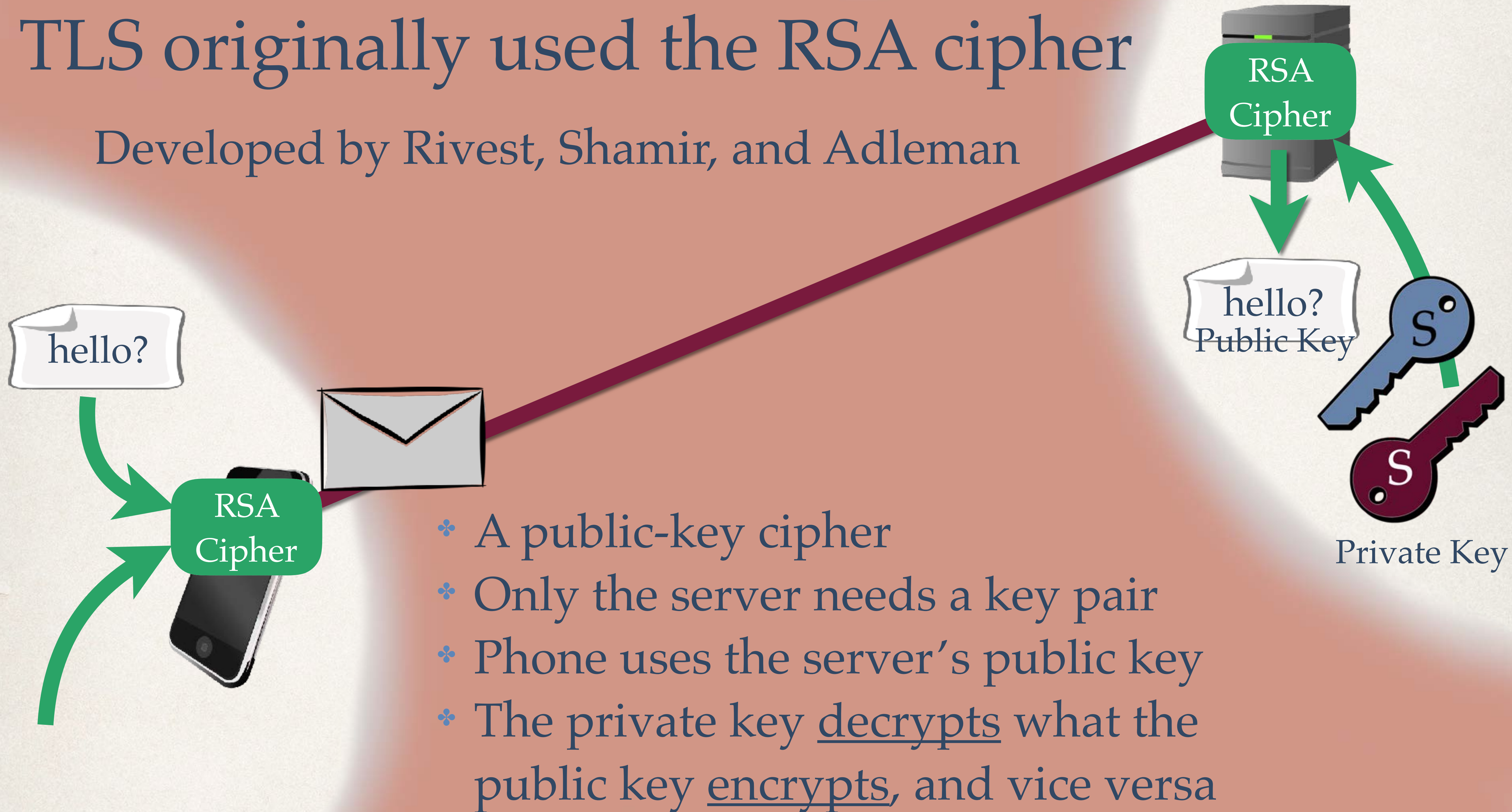
Old-School SSL/TLS Using the RSA Cipher

Cryptosmith Video Series #10

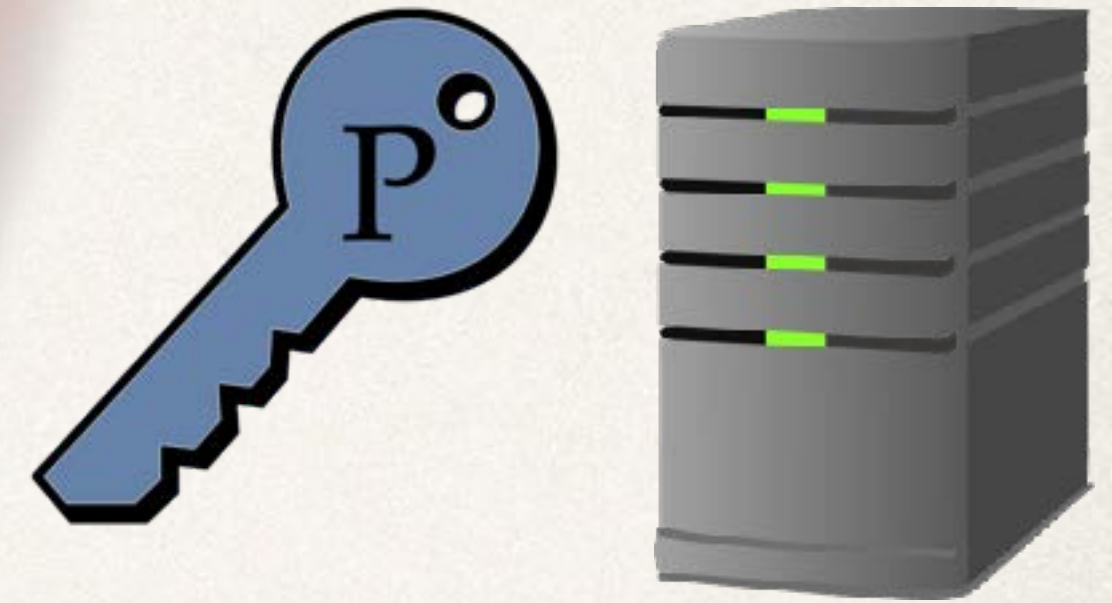
Rick Smith, April, 2017

TLS originally used the RSA cipher

Developed by Rivest, Shamir, and Adleman



Public Key Exchange replaces RSA



- ❖ Elliptic Curve in particular
 - ❖ It is more efficient
 - ❖ It is subtly more secure

- ❖ “Perfect Forward Secrecy” prevents a disclosed secret from uncovering earlier messages
- ❖ RSA remains popular and widely used with TLS



The TLS Protocol using RSA instead of Public Key Exchange

4 Steps

1. Server acquires a public key pair
2. Use public-key crypto to establish a shared secret

3. Use the shared secret to establish a secure link using a secret-key cipher.

4. Use the secure link to exchange encrypted messages.



Public Key



Private Key



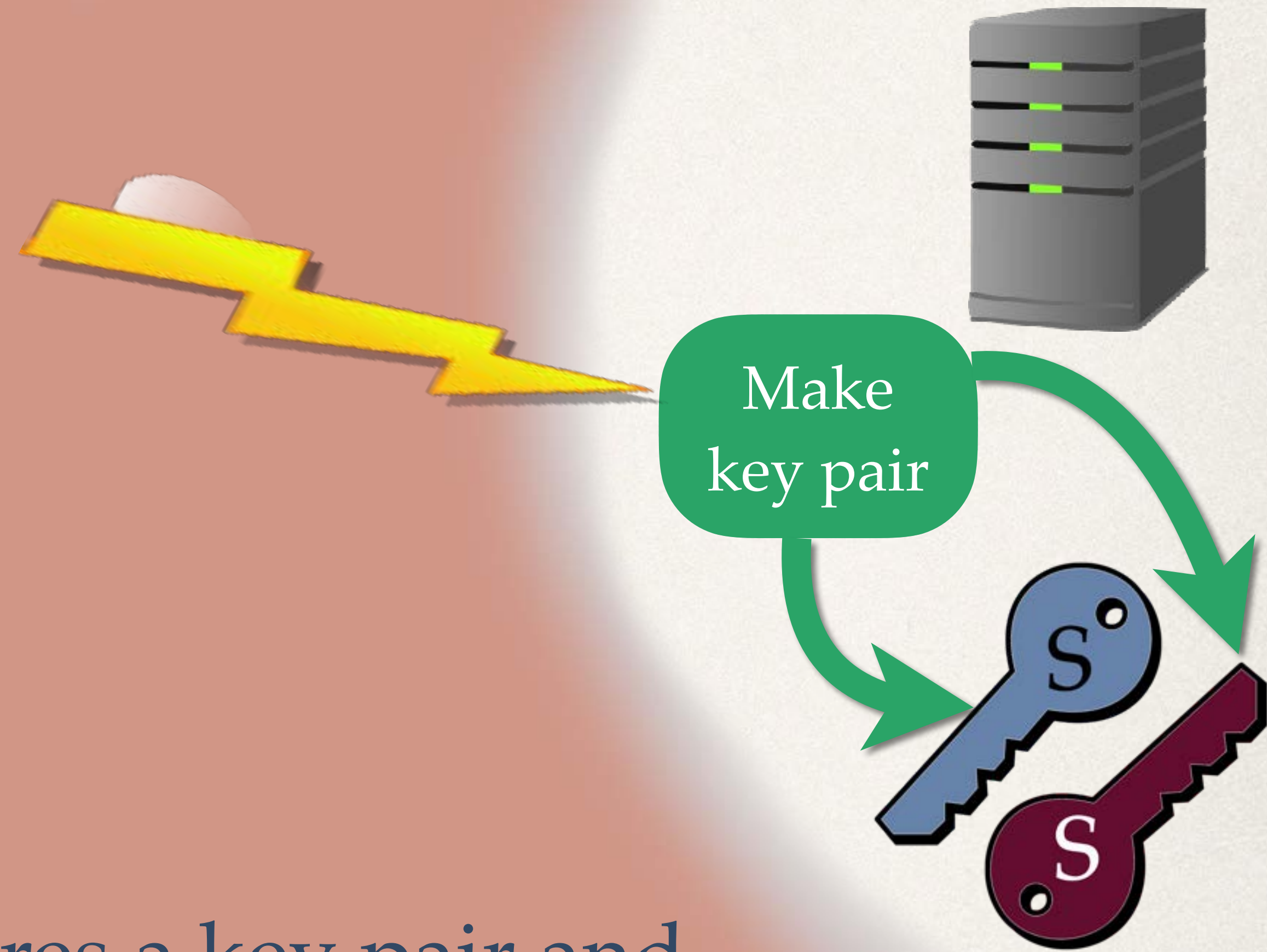
Unchanged

Step 1: Create a key pair

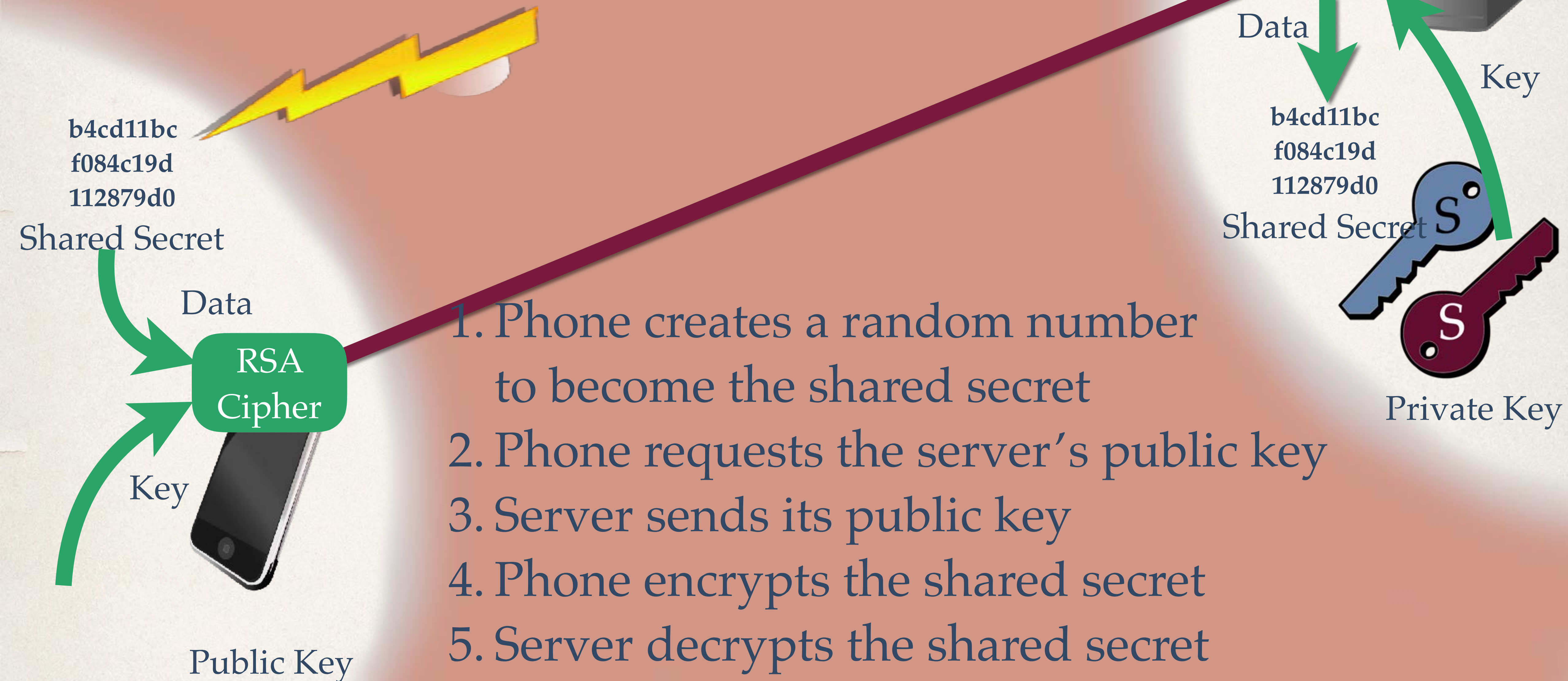
Public Key



- * The server acquires a key pair and uses it for months or years at a time
- * The server shares its public key whenever it opens a TLS connection



Step 2: Establish a shared secret



The RSA Cipher

**MEET AT
THE PARK**

Data

Encrypt

**GZDM WE
CCE JKRF**

Key



Public Key

- * One procedure both encrypts and decrypts
- * Encrypt with one key, decrypt with the other

Private Key



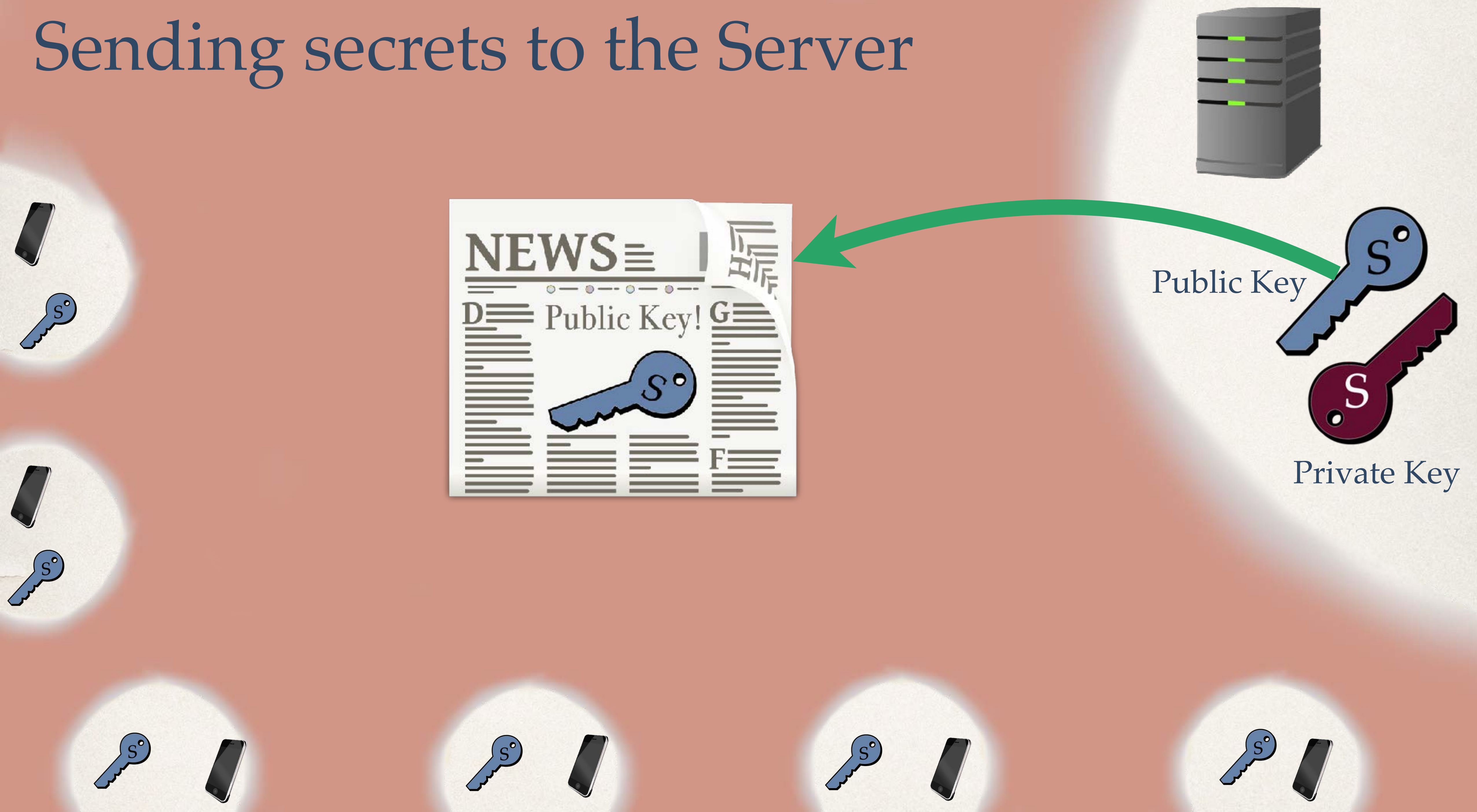
Key

Decrypt

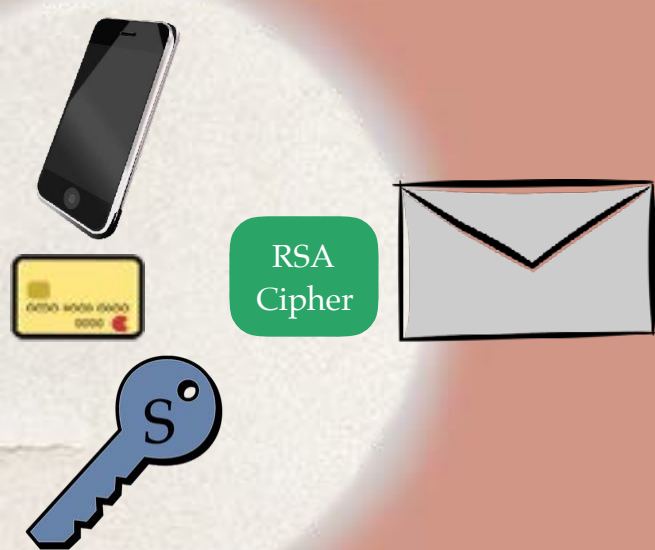
Data

**MEET AT
THE PARK**

Sending secrets to the Server



Sending secrets to the Server



Extracting the Secret Messages



Public Key



Private Key



RSA
Cipher



RSA
Cipher



RSA
Cipher



RSA
Cipher



RSA
Cipher



RSA
Cipher

Using the Public Key Again

**MEET AT
THE PARK**

Data

RSA
Cipher

**GZDM WE
CCE JKRF**

Key



Public Key



Same
Public Key



Key

RSA
Cipher

Data

**PSDO AU
LWG FFKR**
Garbage!

Using the Wrong Private Key

MEET AT
THE PARK

Data

RSA
Cipher

GZDM WE
CCE JKRF

Key



Public Key



Different
Private Key



Key

RSA
Cipher

Data

KLRJ XY
WSH XTSE
Garbage!

Using the Wrong Public Key

**MEET AT
THE PARK**

Data

RSA
Cipher

**GZDM WE
CCE JKRF**

Key



Public Key

Private Key



Key

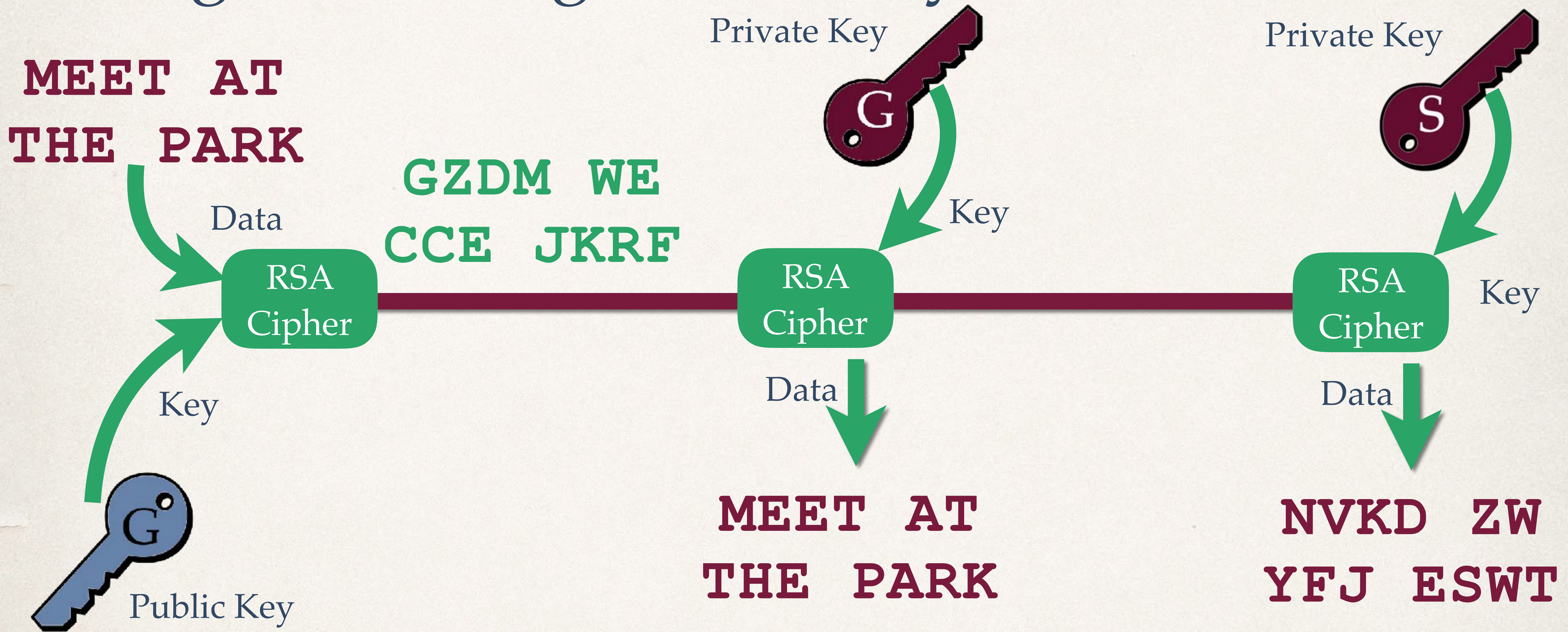
RSA
Cipher

Data

**NVKD ZW
YFJ ESWT**

Garbage!

Using the Wrong Public Key



Solution: Browser Certificates

Identifying Servers With Certificates

Cryptosmith Video Series #11

Rick Smith, March, 2017

ALL

IMAGES

Sign in



● Unknown - Use precise location



https://google.safeid.us

1

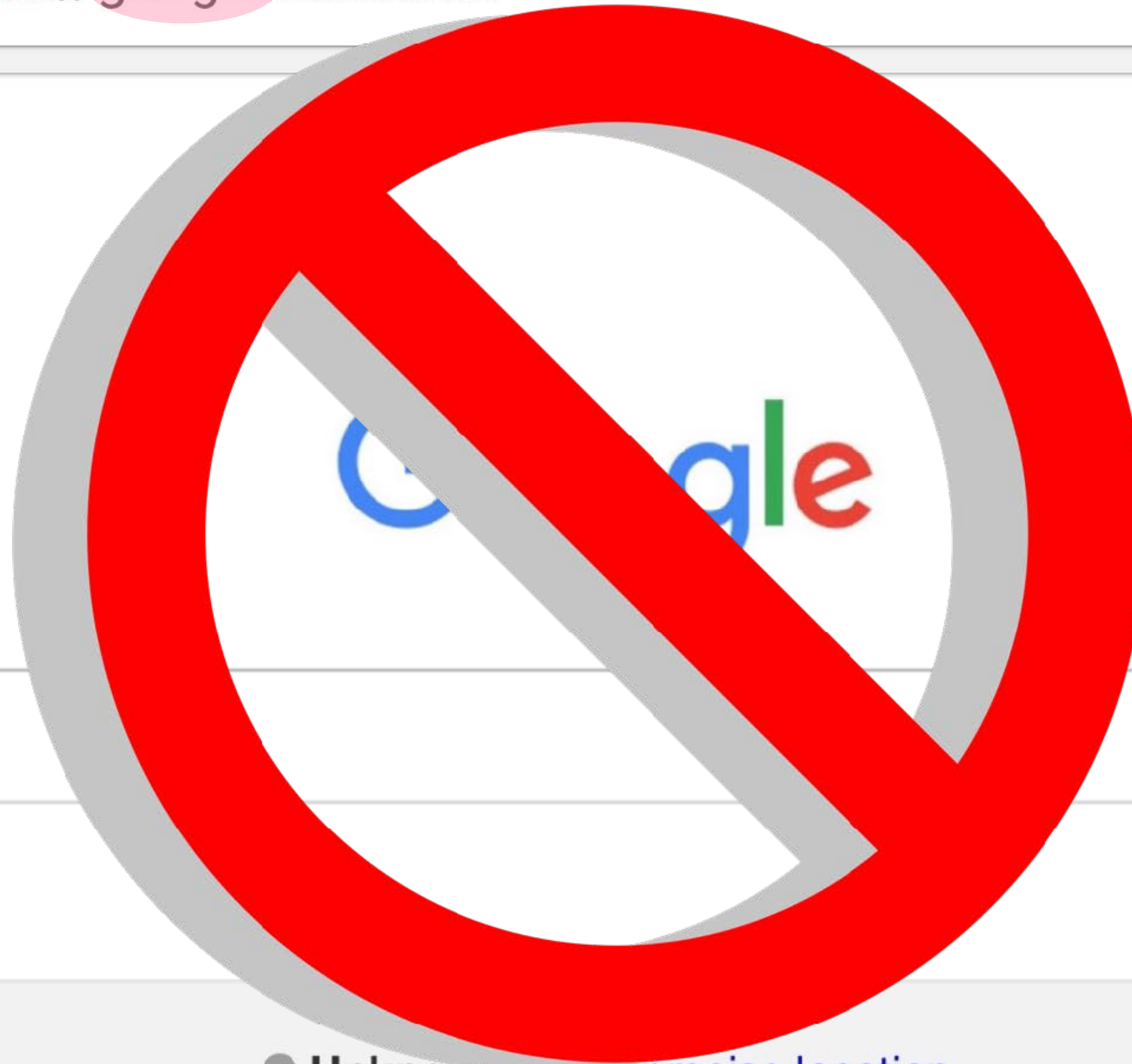


ALL

IMAGES



Sign in





https://www.google.com

1



ALL

IMAGES



Sign in

Google





https://www.google.com

ALL

IMAGES

How does TLS know this is really the Google web site?

Google

Authenticating the Server

Google
web site



?



Public Key



Private Key

1. Did we reach the intended web server?
2. Did we receive the server's public key?

Authenticating the Server



www.google.com



Public-Key Certificate

- ❖ The server's name
- ❖ The server's public key

Authenticating the Server

Google
web site



RSA
Cipher



RSA
Cipher

<https://www.google.com>

1. Client contacts the Server
2. Server sends its certificate
3. Client matches the name
4. Client uses the public key for encryption

Authenticating the Server

Safeid
web site

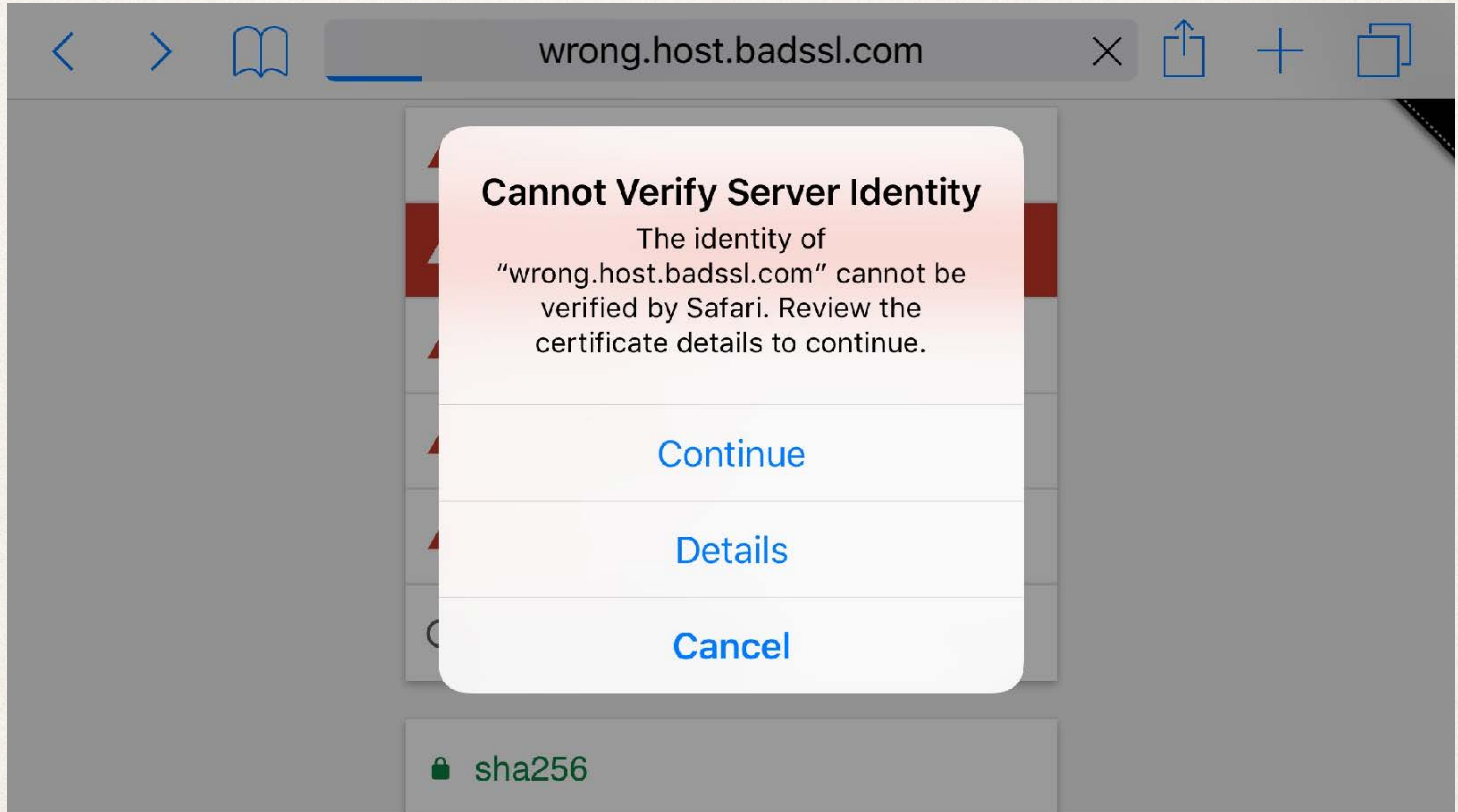


1. Client contacts the Server
2. Server sends its certificate
3. Client matches the name

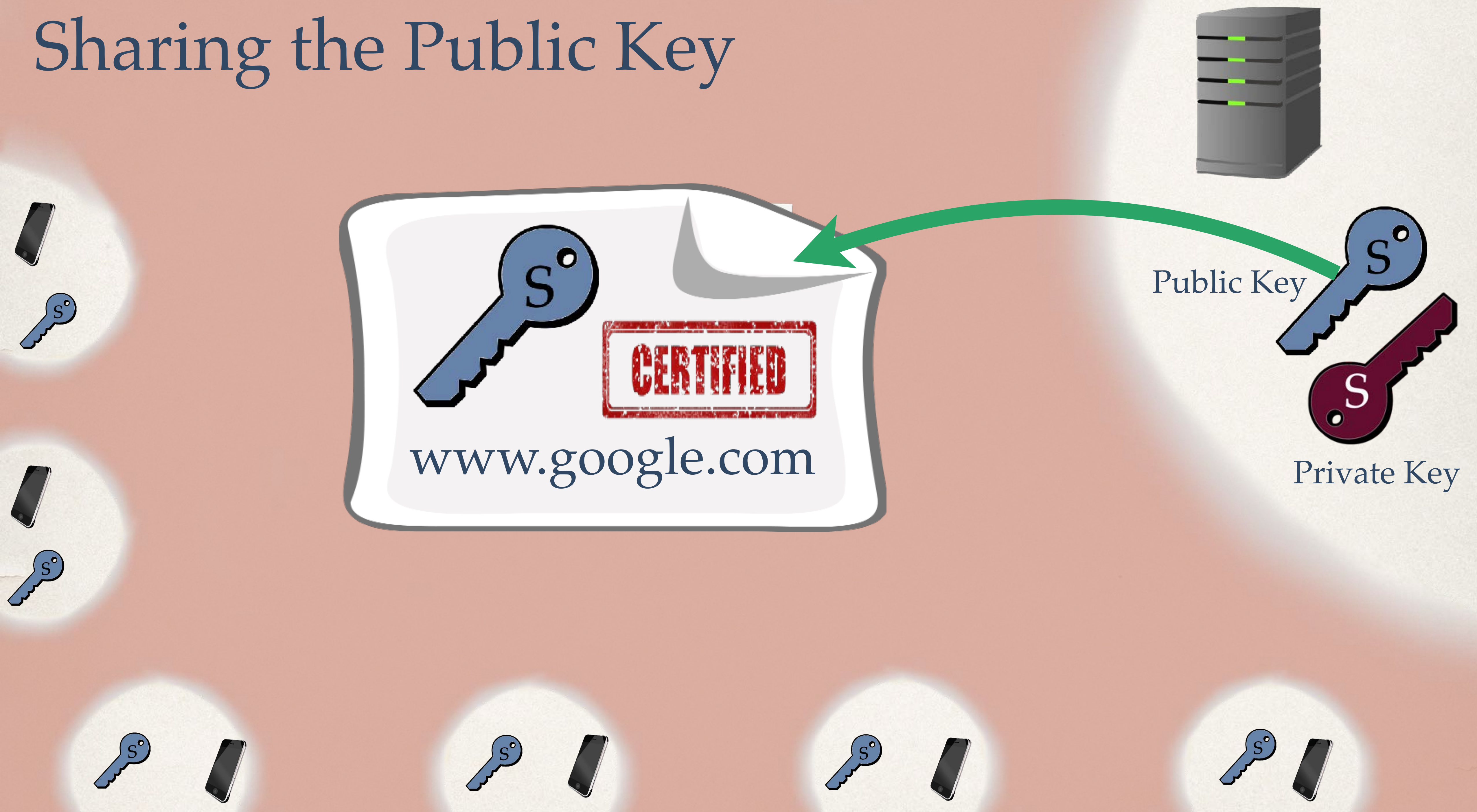


<https://www.google.com>

Authenticating the Server




Sharing the Public Key



A Public-Key Certificate



Reading a Certificate



***.google.com**

Issued by: Google Internet Authority G2

Expires: Wednesday, April 26, 2017 at 8:21:00 AM Central Daylight Time

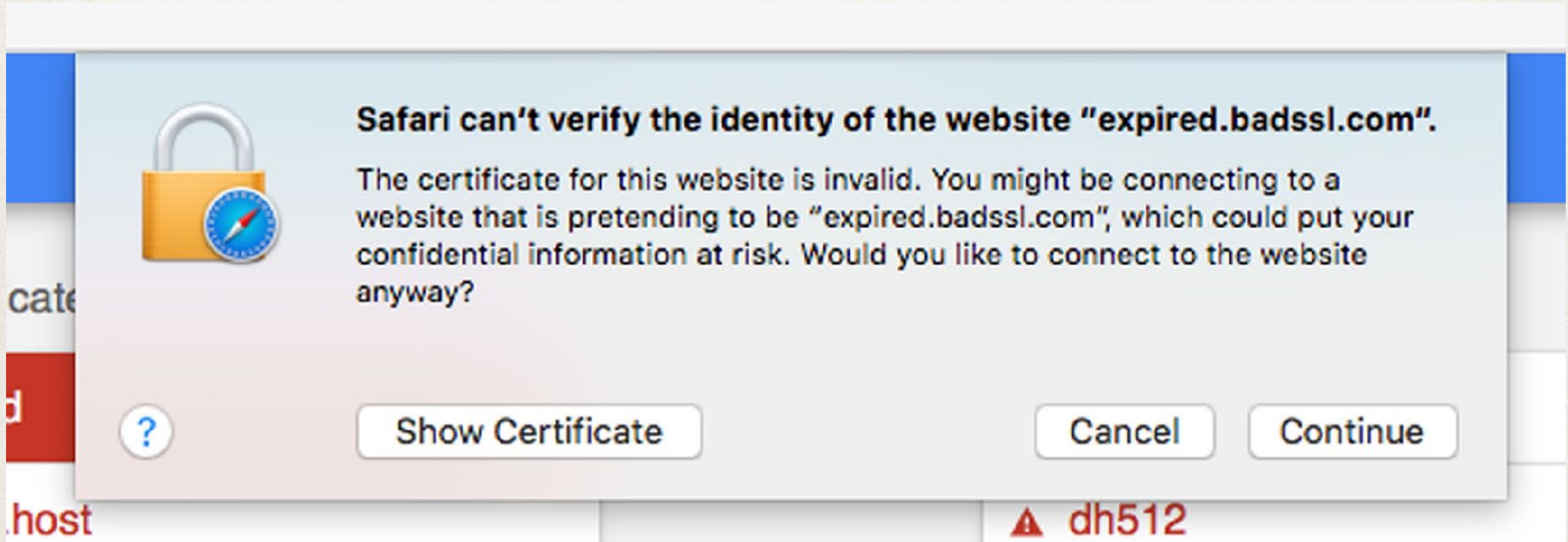
✓ This certificate is valid

▼ **Details**

Subject Name	
Country	US
State/Province	California
Locality	Mountain View
Organization	Google Inc
Common Name	*.google.com

retrieved from a desktop browser

Reading a Certificate - Expired



Reading a Certificate

Serial Number	3821934373800005291
Version	3
Signature Algorithm	SHA-256 with RSA Encryption (1.2.840.113549.1.1.11)
Parameters	none
Not Valid Before	Wednesday, February 1, 2017 at 7:50:27 AM Central Standard Time
Not Valid After	Wednesday, April 26, 2017 at 8:21:00 AM Central Daylight Time
Public Key Info	
Algorithm	Elliptic Curve Public Key (1.2.840.10045.2.1)
Parameters	Elliptic Curve secp256r1 (1.2.840.10045.3.1.7)
Public Key	65 bytes : 04 3D 0F 5D F1 69 3C 81 ...
Key Size	256 bits
Key Usage	Encrypt, Verify, Derive
Signature	256 bytes : 21 3B 42 49 D5 89 C8 C8 ...
Extension	Key Usage (2.5.29.15)
Critical	NO
Usage	Digital Signature
Extension	Basic Constraints (2.5.29.19)
Critical	YES
Certificate Authority	NO
Extension	Extended Key Usage (2.5.29.37)
Critical	NO
Purpose #1	Server Authentication (1.3.6.1.5.5.7.3.1)
Purpose #2	Client Authentication (1.3.6.1.5.5.7.3.2)

DNS Name	g.co
DNS Name	goo.gl
DNS Name	google-analytics.com
DNS Name	google.com
DNS Name	googlecommerce.com
DNS Name	urchin.com
DNS Name	www.goo.gl
DNS Name	youtu.be
DNS Name	youtube.com
DNS Name	youtubeducation.com
Extension	Certificate Policies (2.5.29.32)
Critical	NO
Policy ID #1	(1.3.6.1.4.1.11129.2.5.1)
Policy ID #2	(2.23.140.1.2.2)
Extension	CRL Distribution Points (2.5.29.31)
Critical	NO
URI	http://pki.google.com/GIAG2.crl
Extension	Certificate Authority Information Access (1.3.6.1.5.5.7.1.1)
Critical	NO
Method #1	CA Issuers (1.3.6.1.5.5.7.48.2)
URI	http://pki.google.com/GIAG2.crt
Method #2	Online Certificate Status Protocol (1.3.6.1.5.5.7.48.1)
URI	http://clients1.google.com/ocsp
Fingerprints	
SHA1	FA A0 23 97 AB E7 F7 65 53 14 A3 B6 D4 1F 67 5C 4D B7 BD 83
MD5	62 AF 77 0A B4 B7 D8 CE 46 2C 36 8B C4 84 F6 1E

Reading a Certificate

Public Key 65 bytes : 04 3D 0F 5D F1 69 3C 81 C6 A1 B3 DC 45 07 B9 EF 09 D6 92 80 9A 9C 3F 13 AE 1A 4B 39
0E 74 72 C1 15 85 5B 85 5C 02 BF 2E CB 6B 4C 02 73 1C 21 FB 8D D8 C3 B3 86 C4 ED 1B F7 AC A4
28 9D 8F 9D 4B 51

Key Size 256 bits

Key Usage Encrypt, Verify, Derive

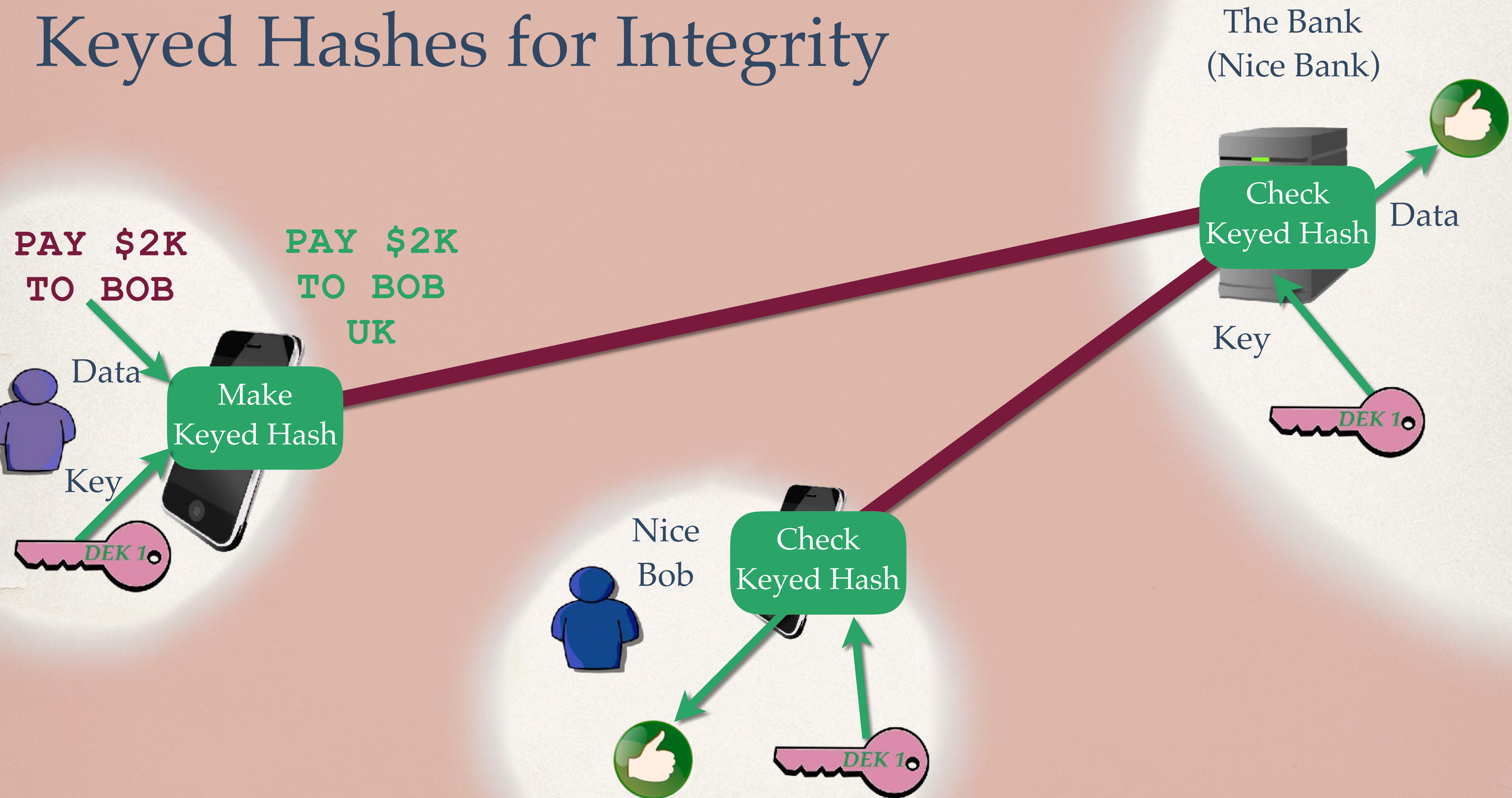
Signature 256 bytes : 21 3B 42 49 D5 89 C8 C8 A9 94 35 ED 11 2B ED 8C BF 6B 5E F7 6E 03 5E FE AA 79 0C 74
57 D1 F6 09 97 54 E4 CC 99 30 DA 29 2A F1 C8 47 93 87 70 D3 6B C1 BE 45 55 B3 78 0A 00 C4 31
74 BE 55 BC 0E 01 69 59 8A C6 E6 83 8C E5 4B 1F F7 86 05 E1 E9 0E A1 63 1B 23 6A FA 0F 33 50 49
E7 9C 68 3A 3F 78 A8 1A 21 42 B3 FA 0C 0B 60 55 2A FF 89 6A F8 05 2F C5 B1 D1 4A 92 32 27 D4 A0
A5 5D 14 FF 08 E2 57 68 85 C3 2E 04 01 16 B9 25 B4 32 E8 A9 CB 5A 6A 70 B2 DC 69 B2 61 6B 9A
DA B5 0F 0A 7A 91 9B F4 68 43 DF 08 17 7F AA BD 01 EE 01 81 7C 53 17 06 6A C6 4E 34 A3 3B 8C 0A
3A 15 27 9B EF 42 E9 E5 39 3E 9A 8A 0A 91 13 23 04 41 E2 40 73 C1 A2 F3 7D 35 9F 3F 32 D8 A7 51
DD 88 2D B8 57 A8 C9 51 00 1E EF 56 F4 F8 3B AA 4C 33 0F 3B ED 8F C8 E9 26 5A 4D 98 54 C2 9C
A9 CF BF DF C8 26 F6

Digital Signatures

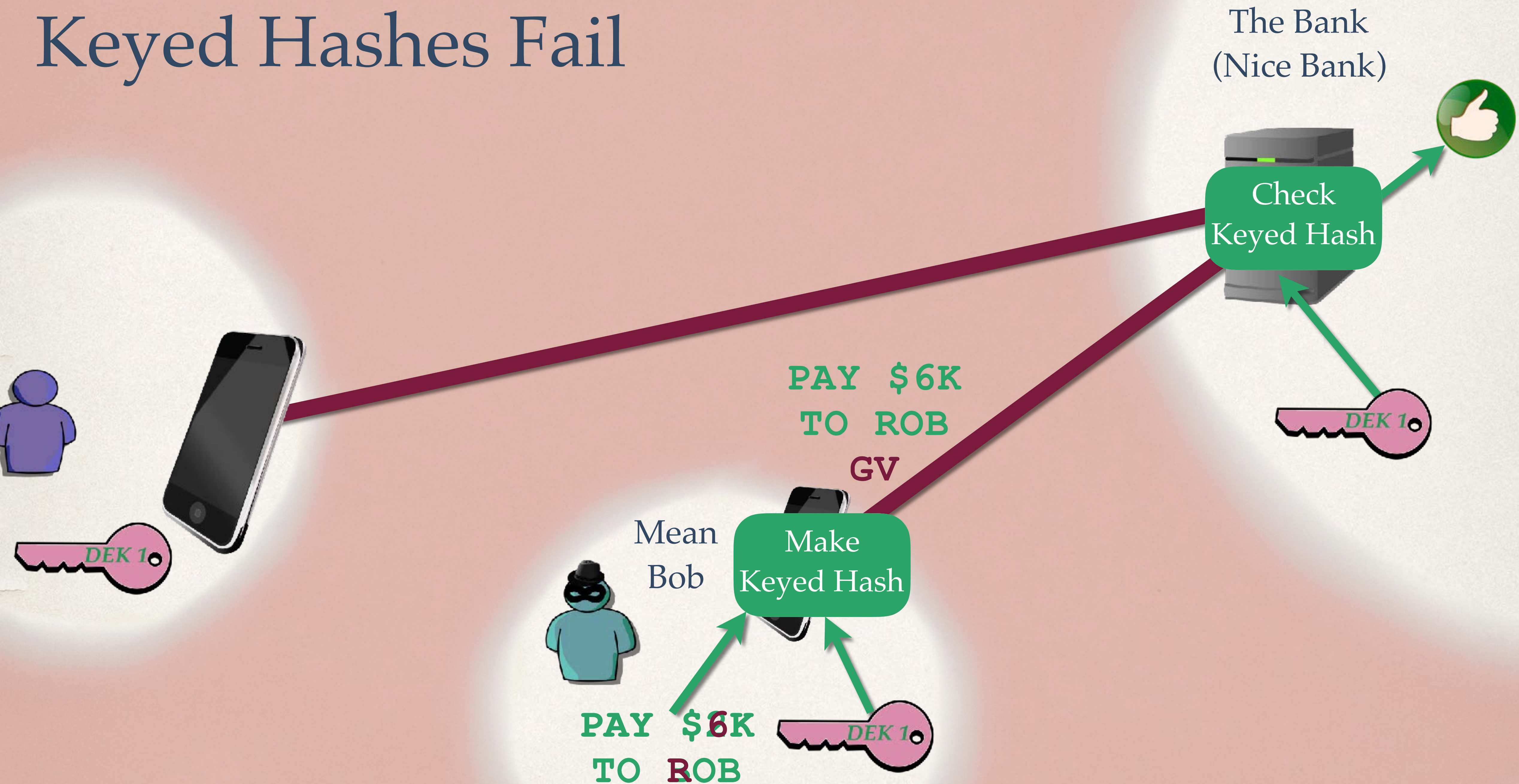
Cryptosmith Video Series #12

Rick Smith, April, 2017

Keyed Hashes for Integrity



Keyed Hashes Fail



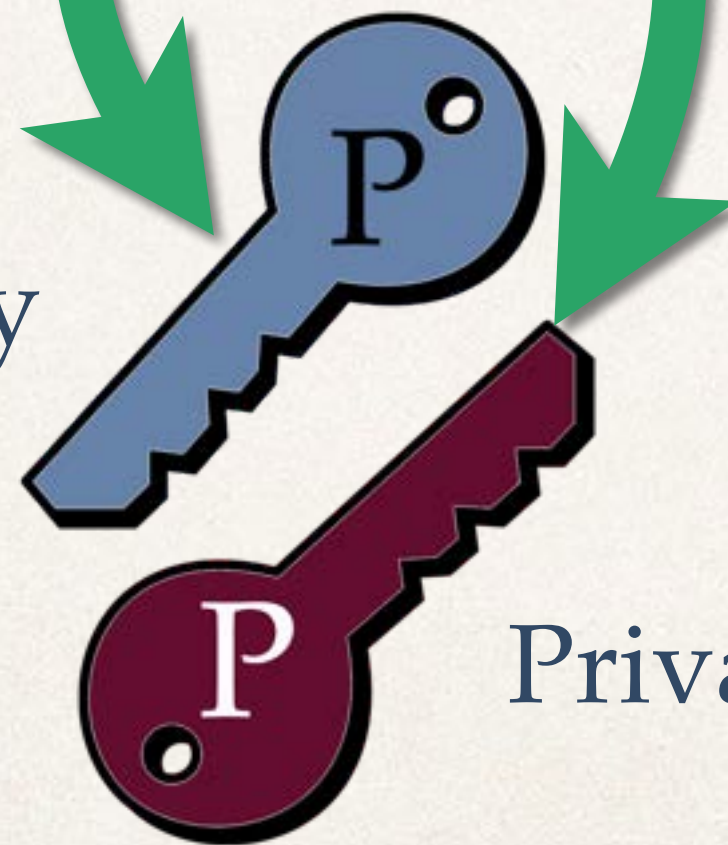
Digital Signatures

The Bank

PAY \$2K
TO BOB



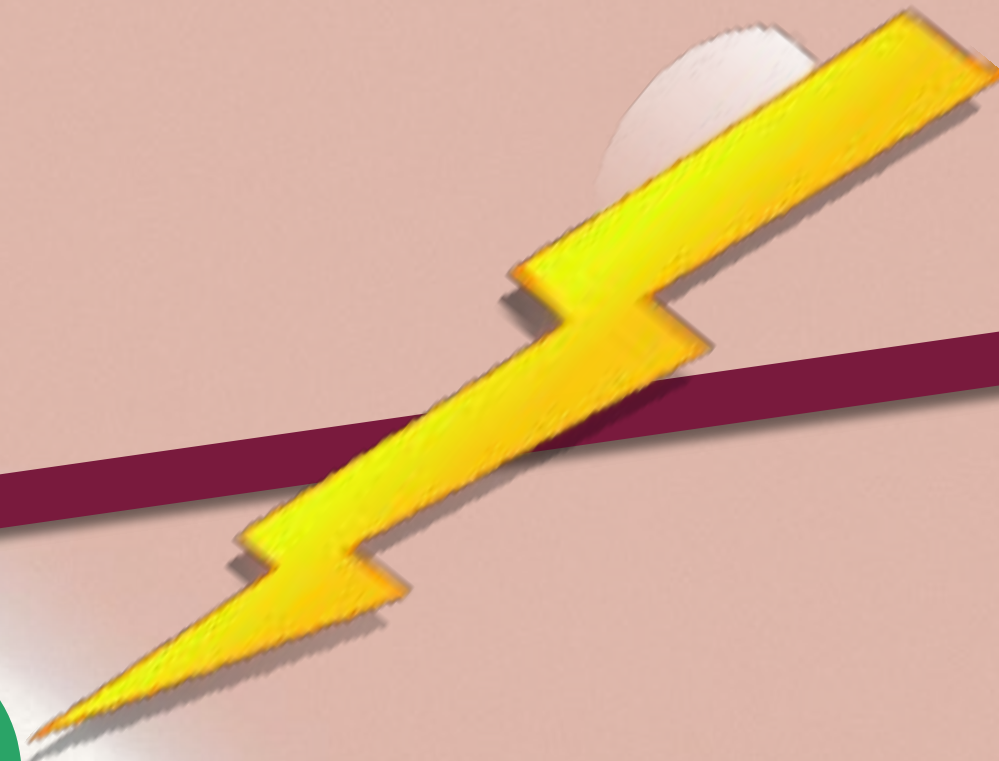
Public Key



Private Key

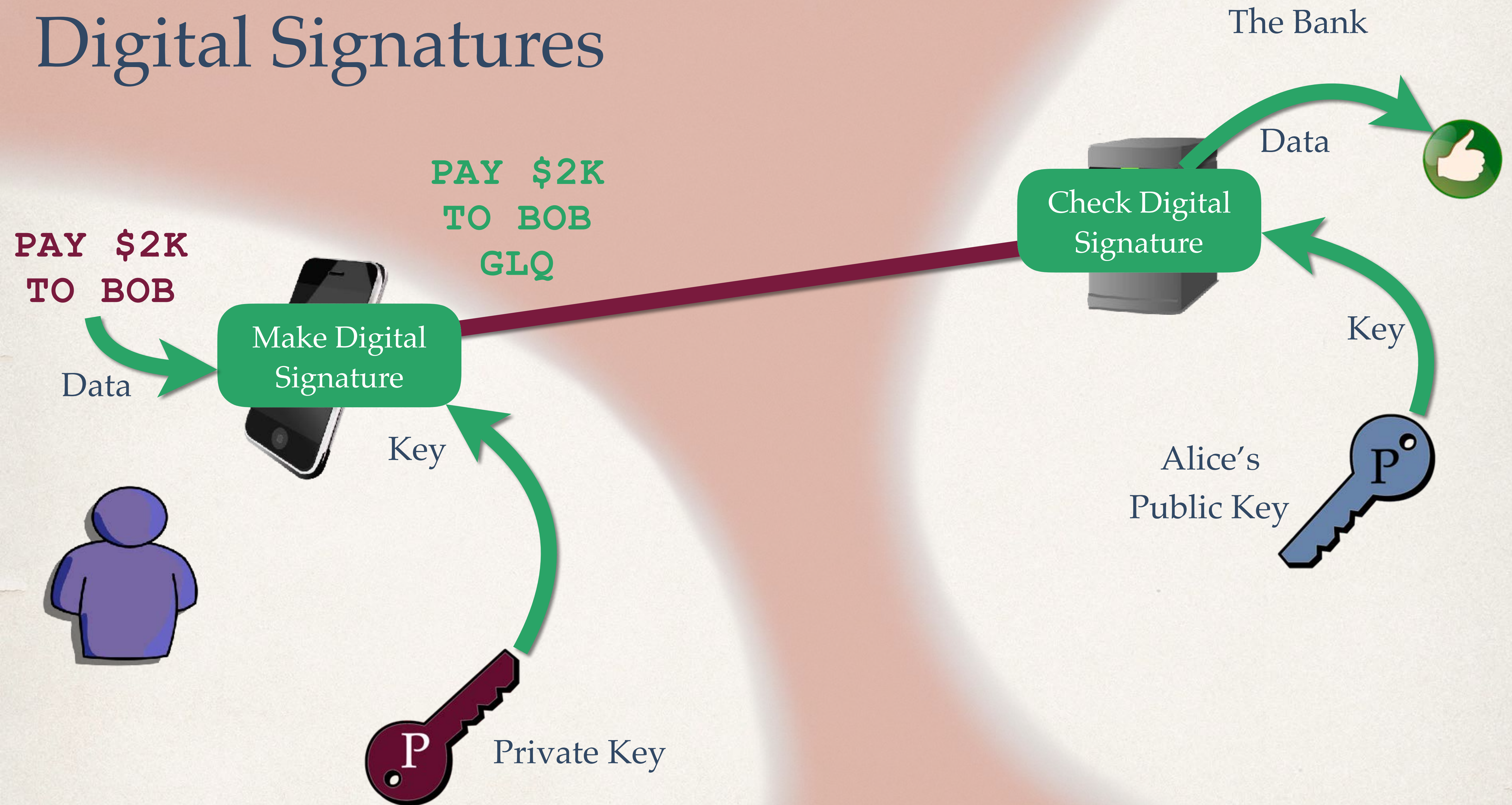


Make
key pair

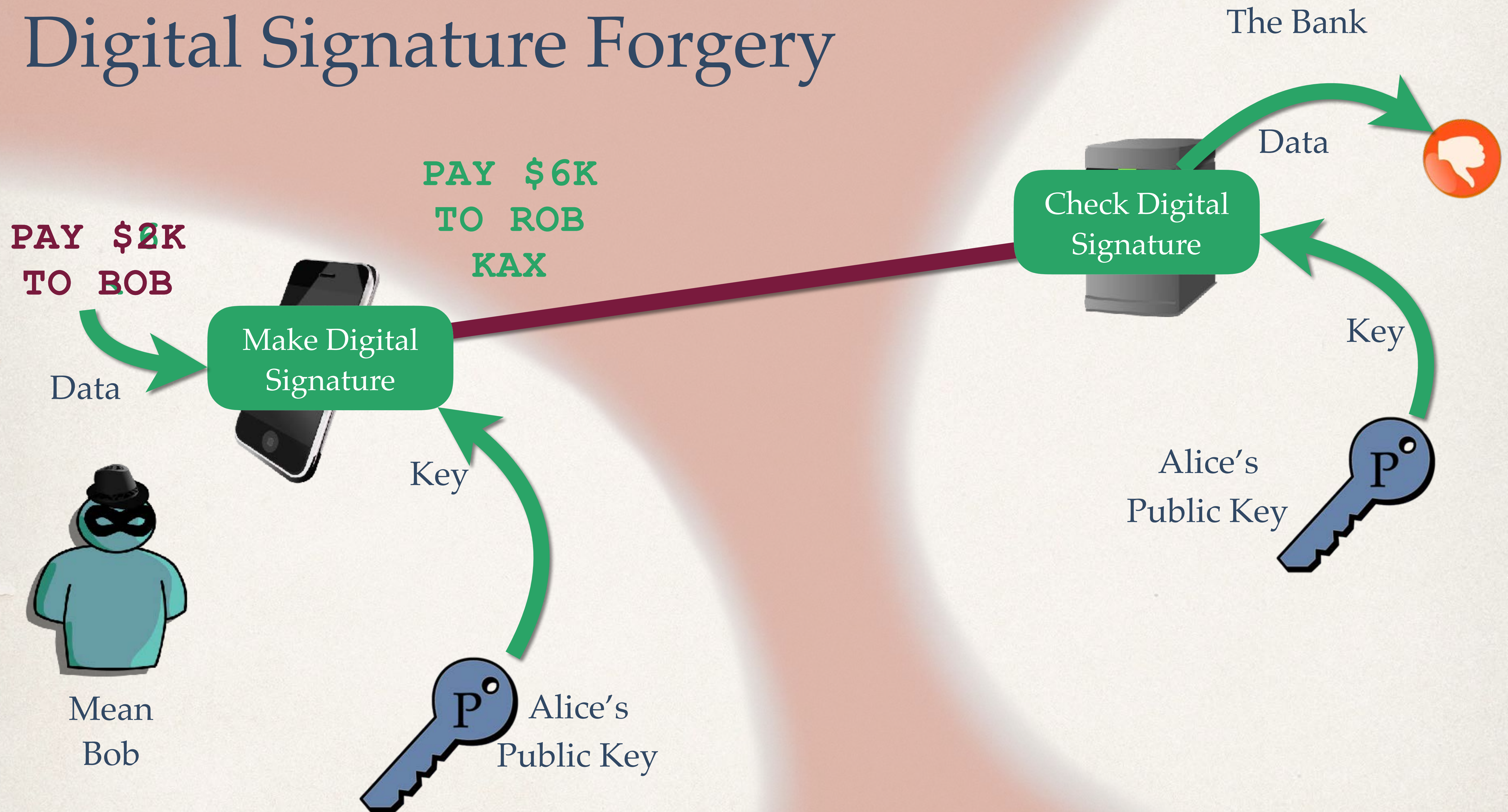


Alice's

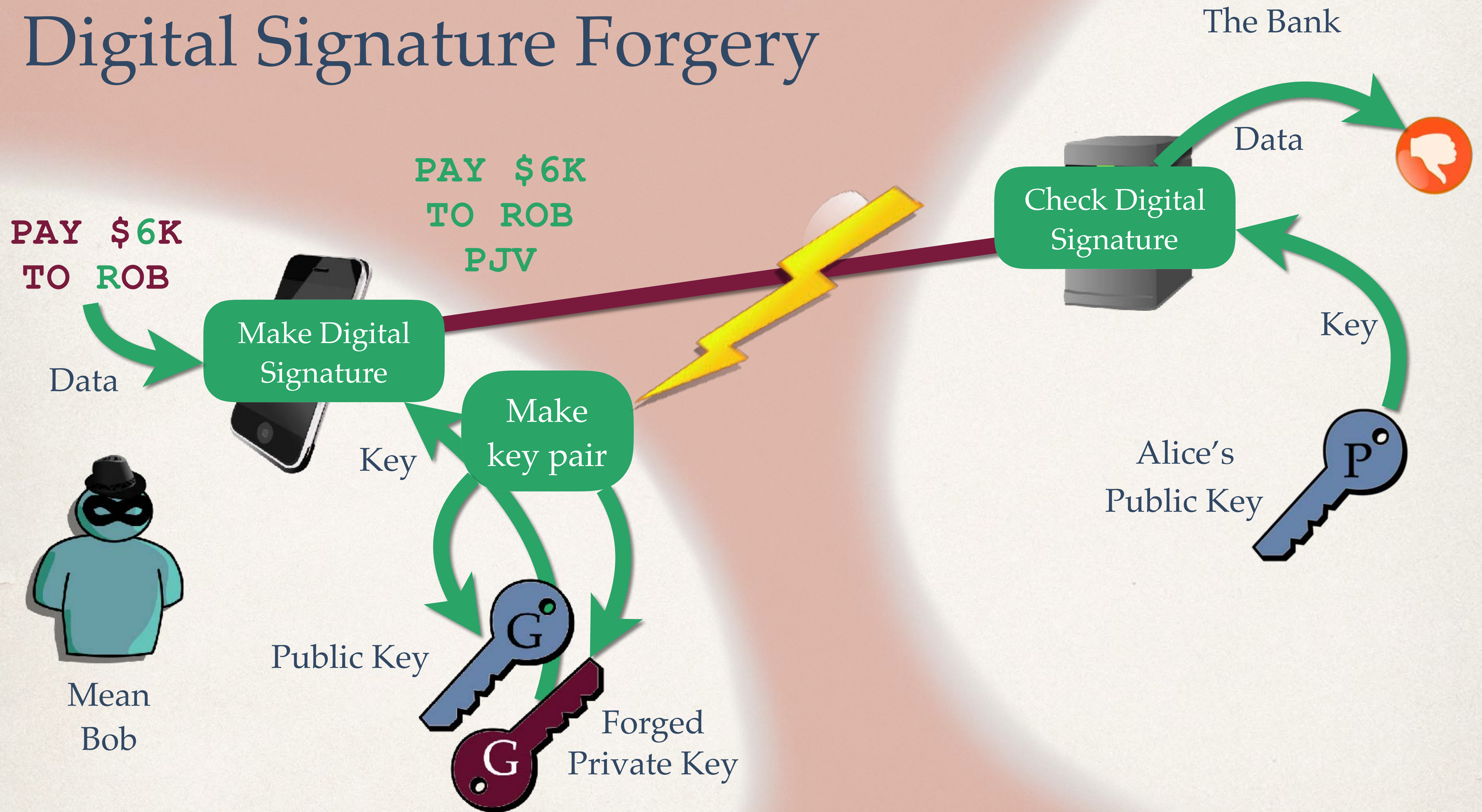
Digital Signatures



Digital Signature Forgery



Digital Signature Forgery



Digital Signature Forgery

Alice



Public Key

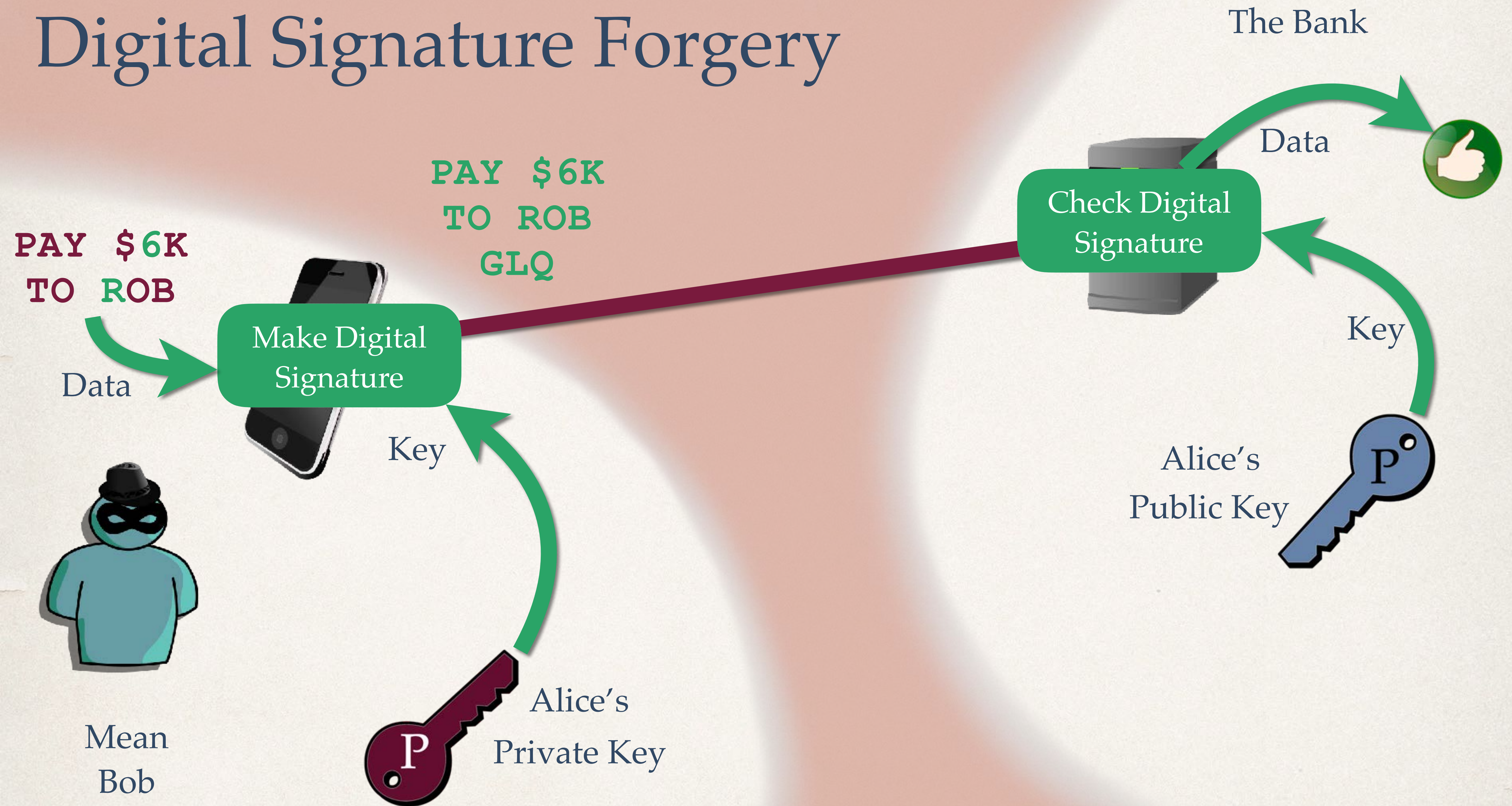


Private Key

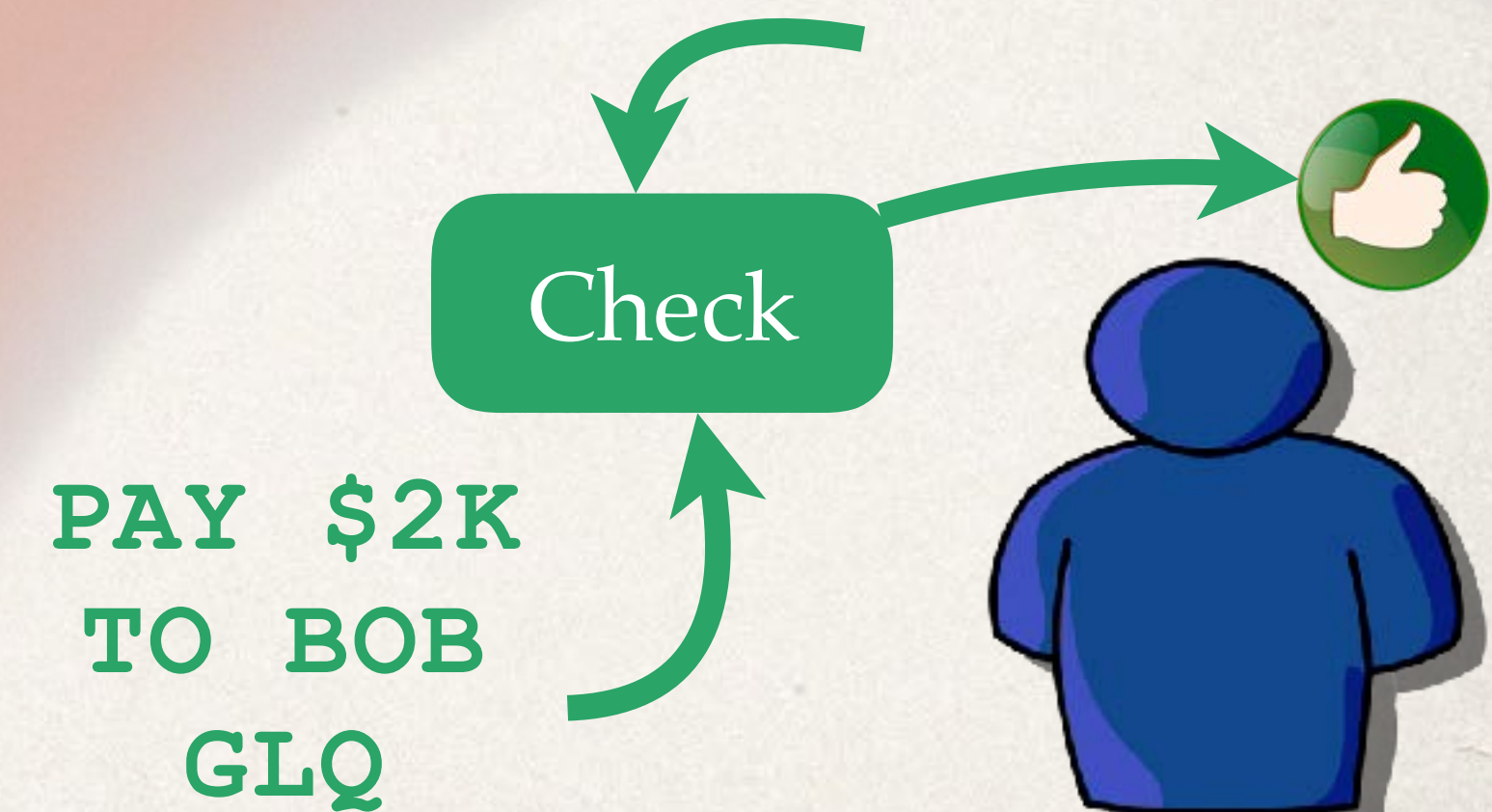
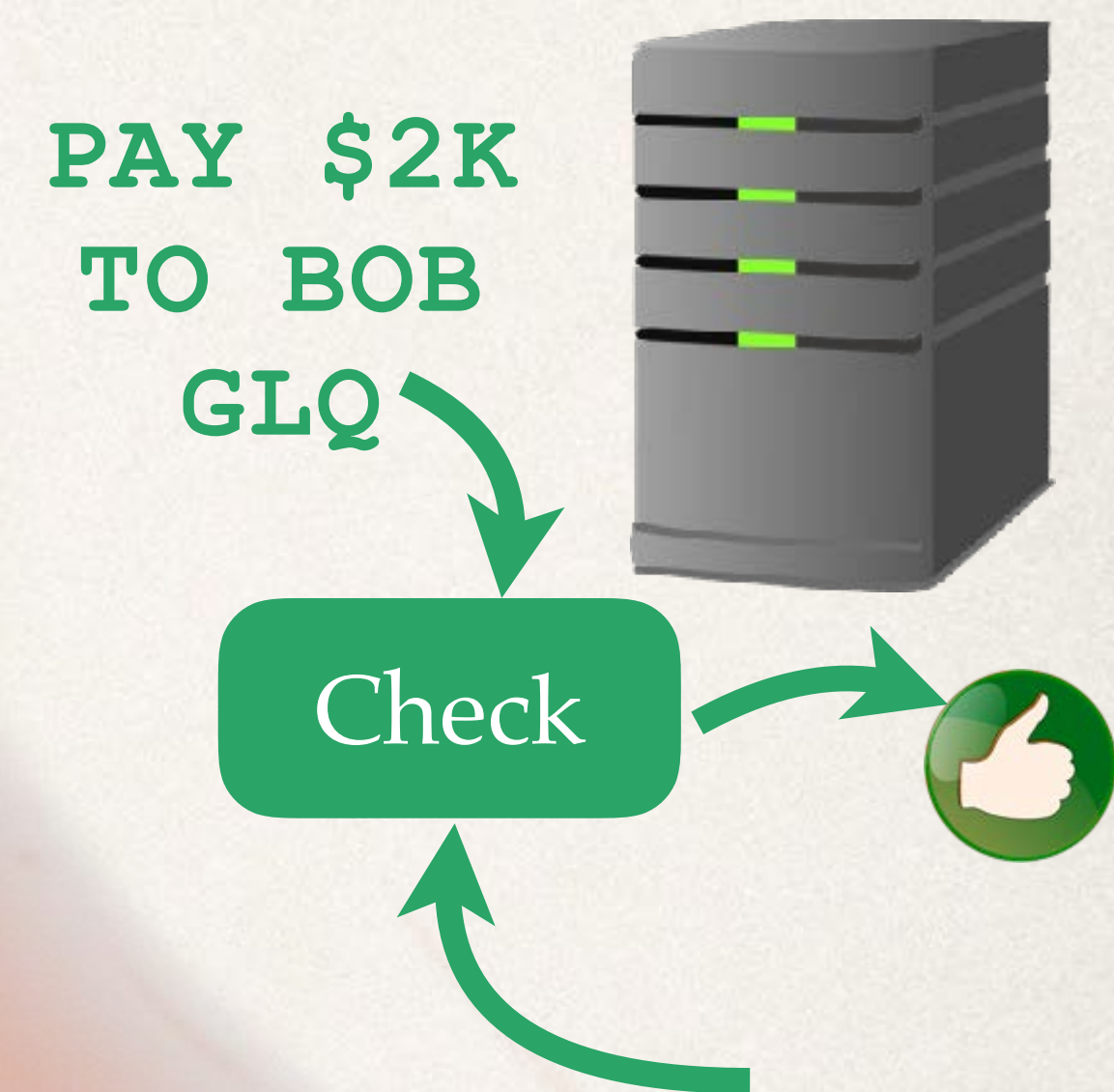
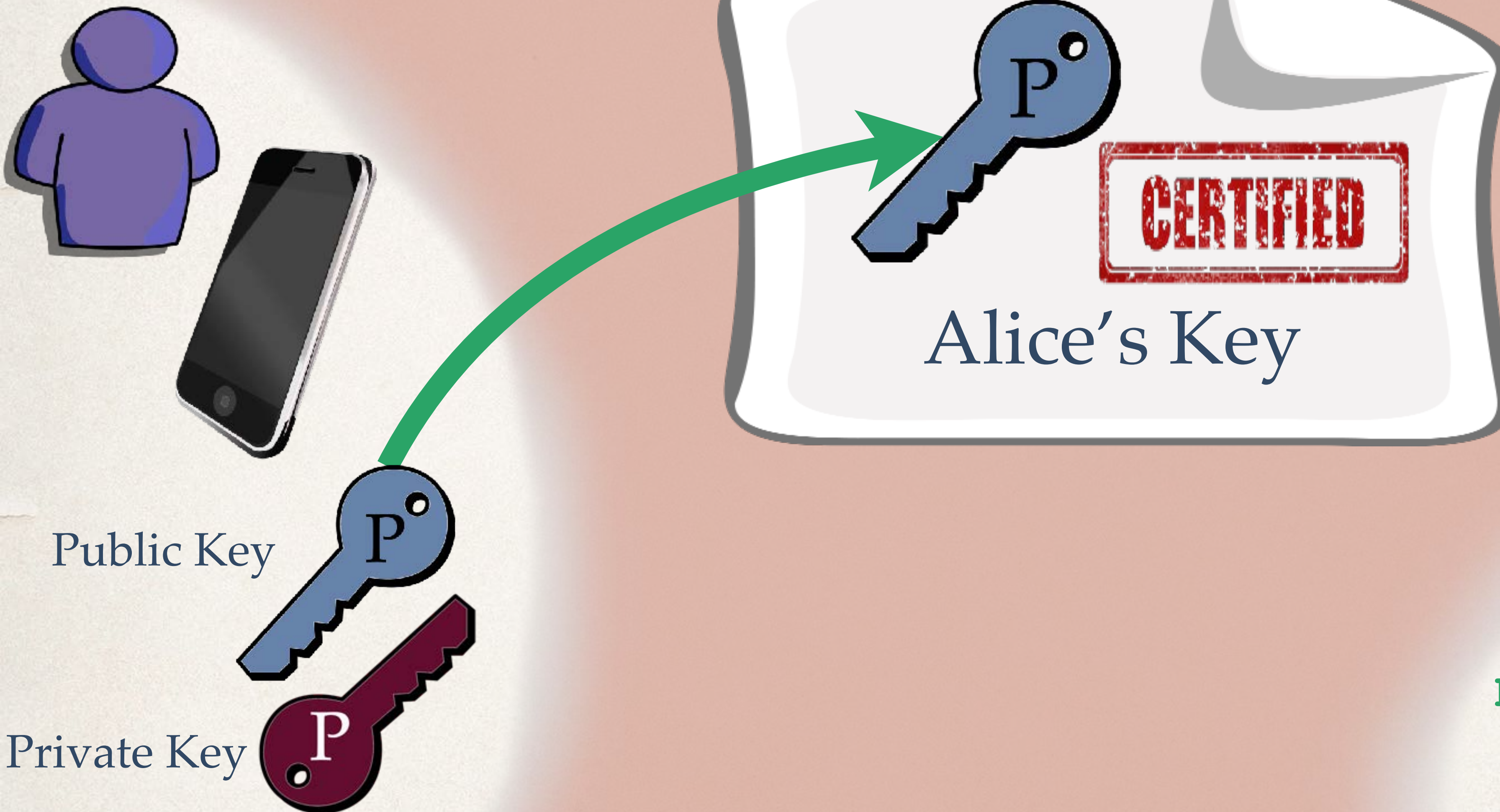


Mean
Bob

Digital Signature Forgery



Sharing a Public Key



Validating a Public- Key Certificate

Cryptosmith Video Series #13

Rick Smith, April, 2017

Authenticating a Server

Google
web site



<https://www.google.com>

A Public-Key Certificate



Certificate Ownership and Validity



*.google.com

Issued by: Google Internet Authority G2

Expires: Wednesday, April 26, 2017 at 8:21:00 AM Central Daylight Time

✓ This certificate is valid

▼ Details

Subject Name

Country	US
State/Province	California
Locality	Mountain View
Organization	Google Inc
Common Name	*.google.com

Owner's
(web site)
Name

Who
Signed the
Certificate

Certificate
Expiration
Date

Contents of a Certificate

Public Key 65 bytes : 04 3D 0F 5D F1 69 3C 81 C6 A1 B3 DC 45 07 5D 9A 9C 3F 13 AE 1A 4B 39
0E 74 72 C1 15 85 5B 85 5C 02 BF 2E CB 6B 4C 3B B3 86 C4 ED 1B F7 AC A4
28 9D 8F 9D 4B 51

Key Size 256 bits

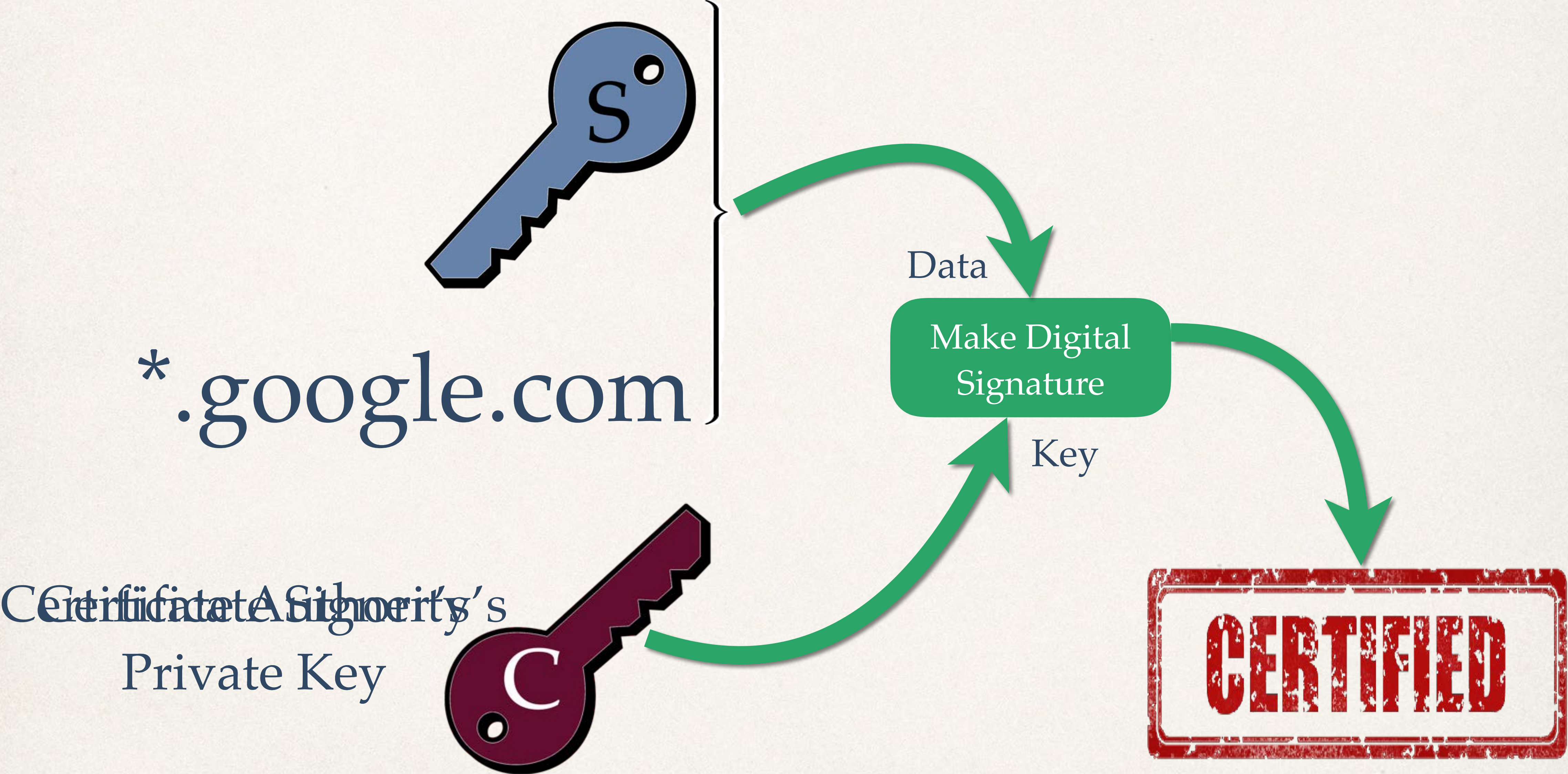
Key Usage	Encrypt, Verify, Derive
<ul style="list-style-type: none"> • Asymmetric <ul style="list-style-type: none"> • Public Key <ul style="list-style-type: none"> • Encryption • Signature Verification • Private Key <ul style="list-style-type: none"> • Decryption • Signature Generation • Symmetric <ul style="list-style-type: none"> • Encryption • Decryption 	<ul style="list-style-type: none"> • Asymmetric <ul style="list-style-type: none"> • Key Agreement • Symmetric <ul style="list-style-type: none"> • Key Derivation

CERTIFIED

Public Key

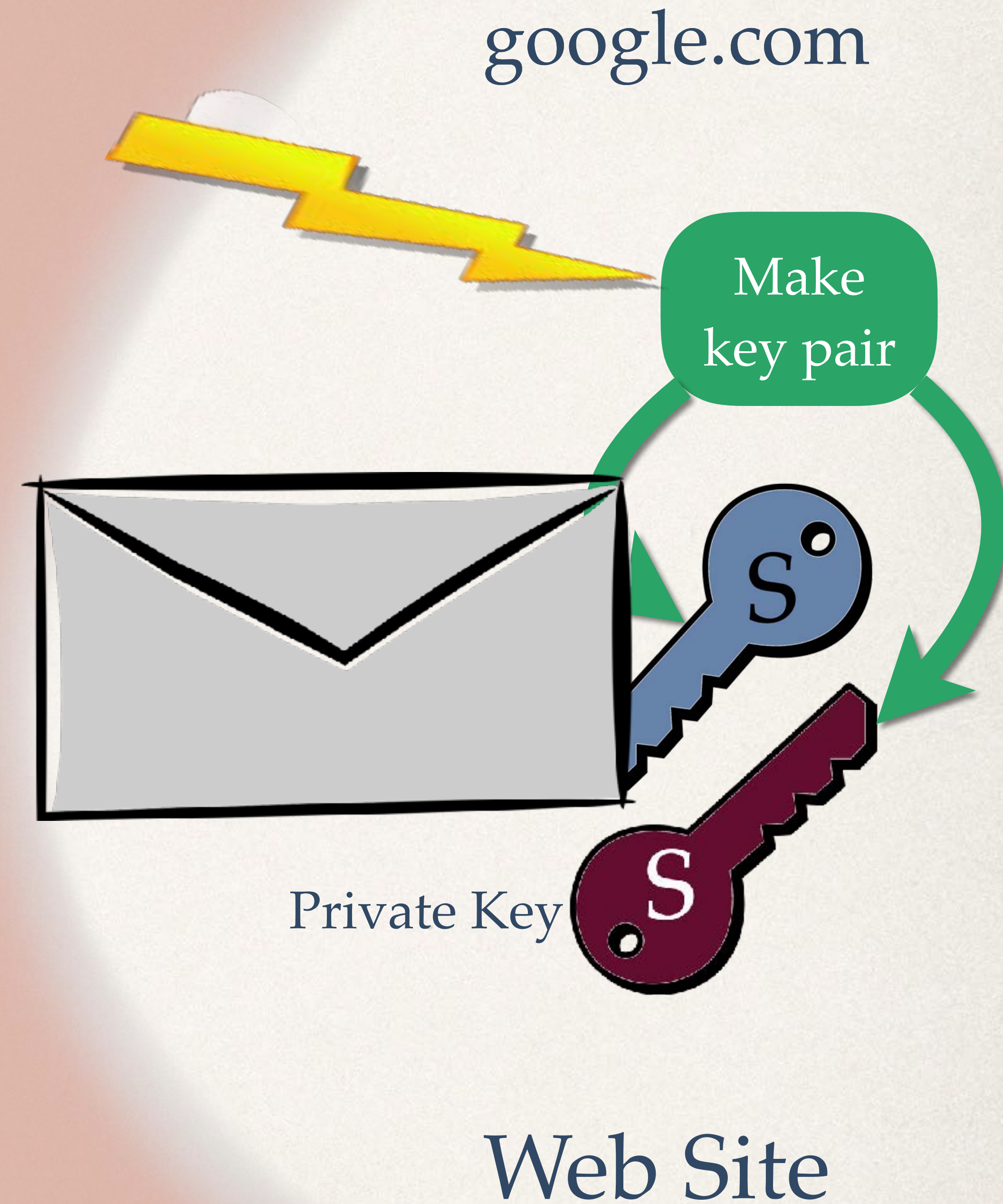
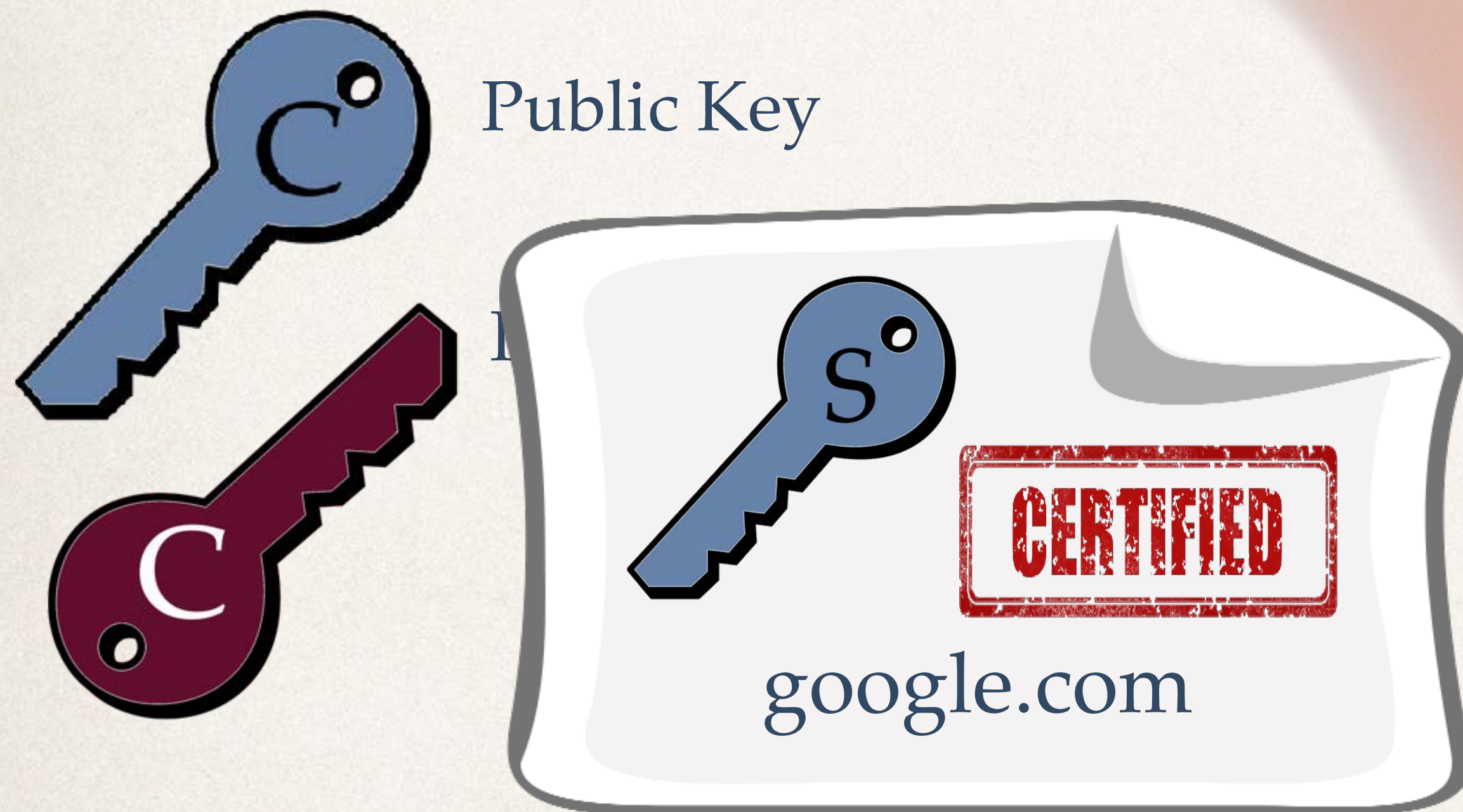
Digital Signature

Signing a Certificate

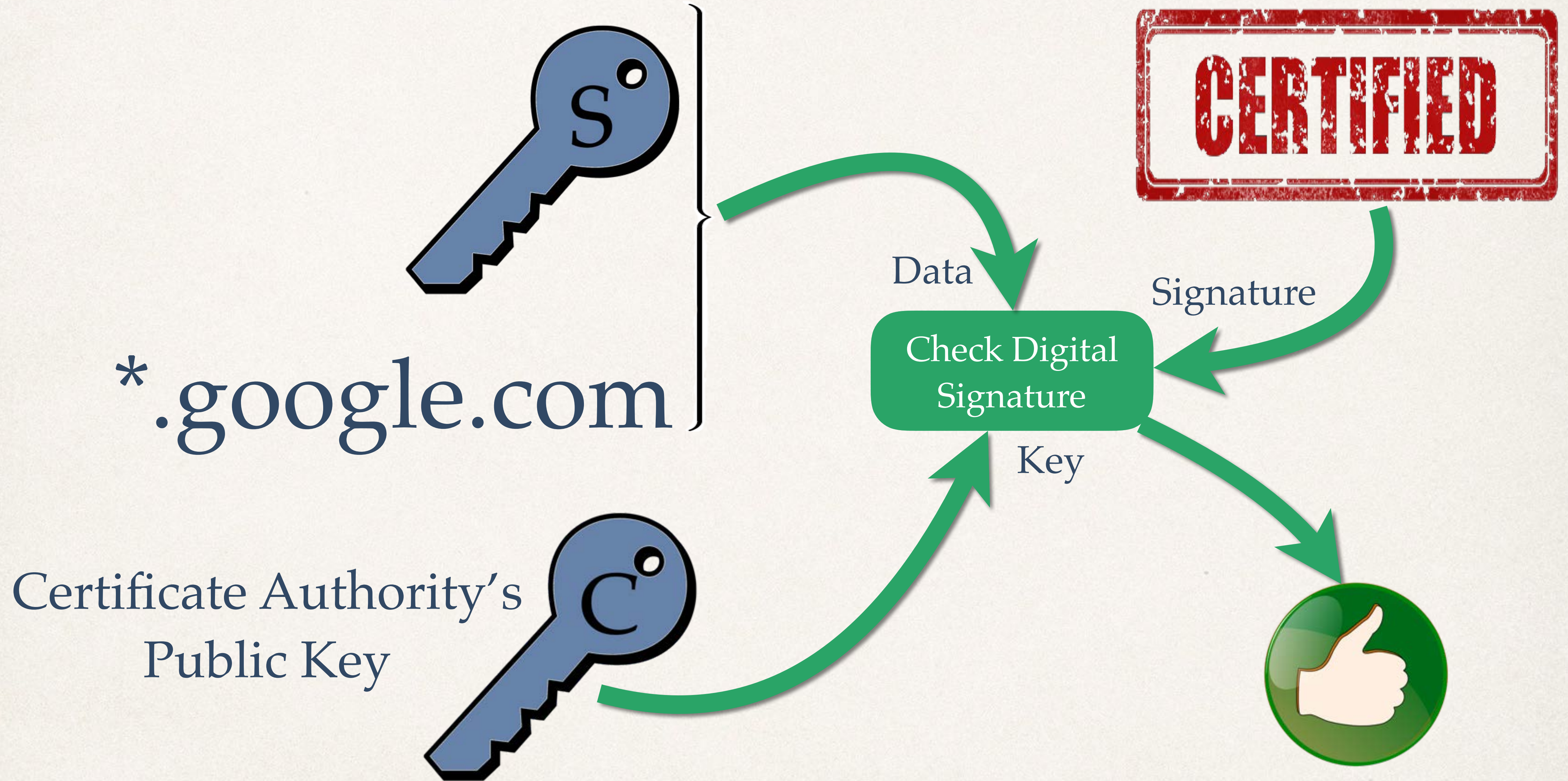


Issuing a Certificate

Certificate Authority



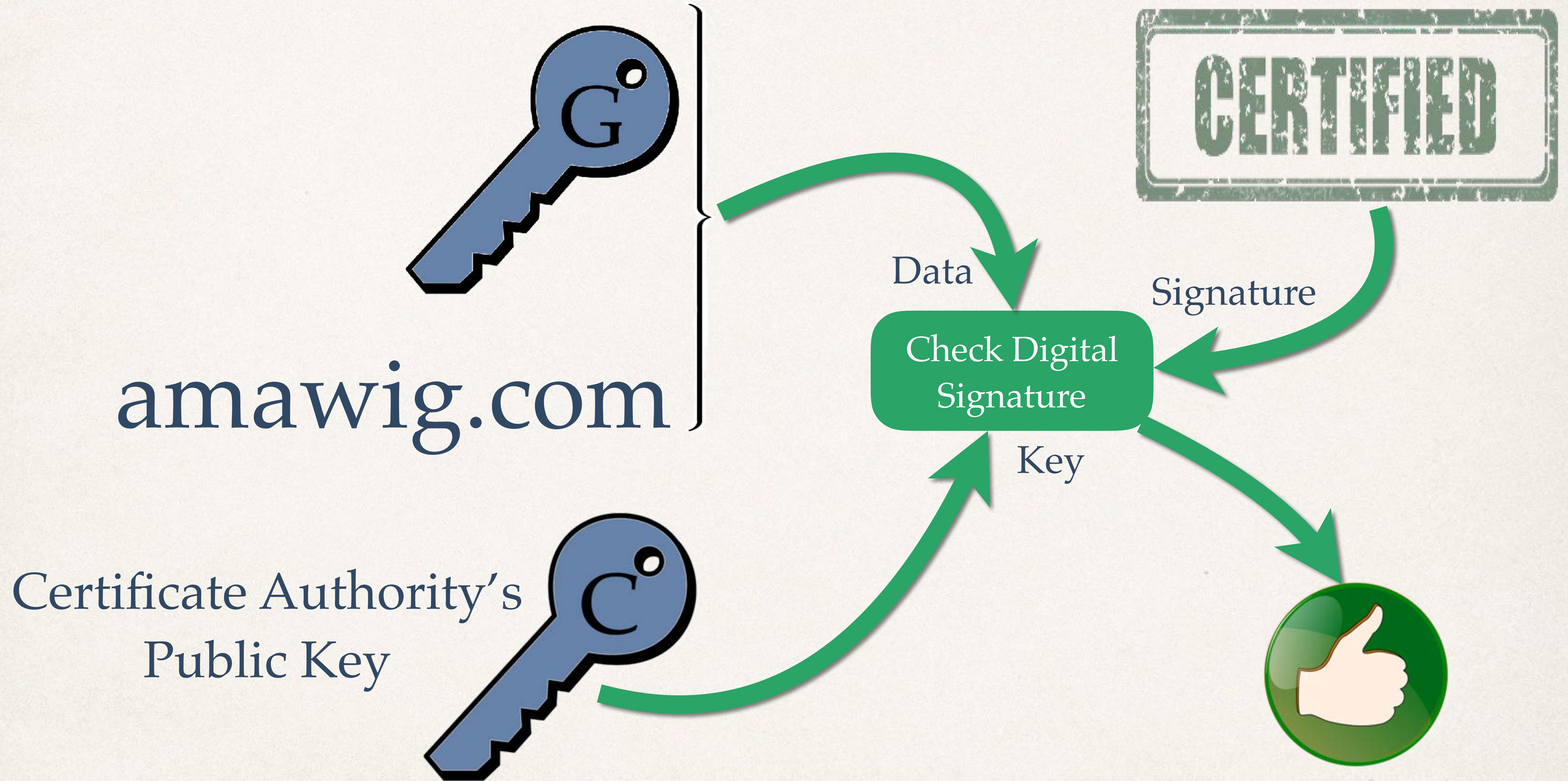
Validating a Certificate



Validating a Certificate



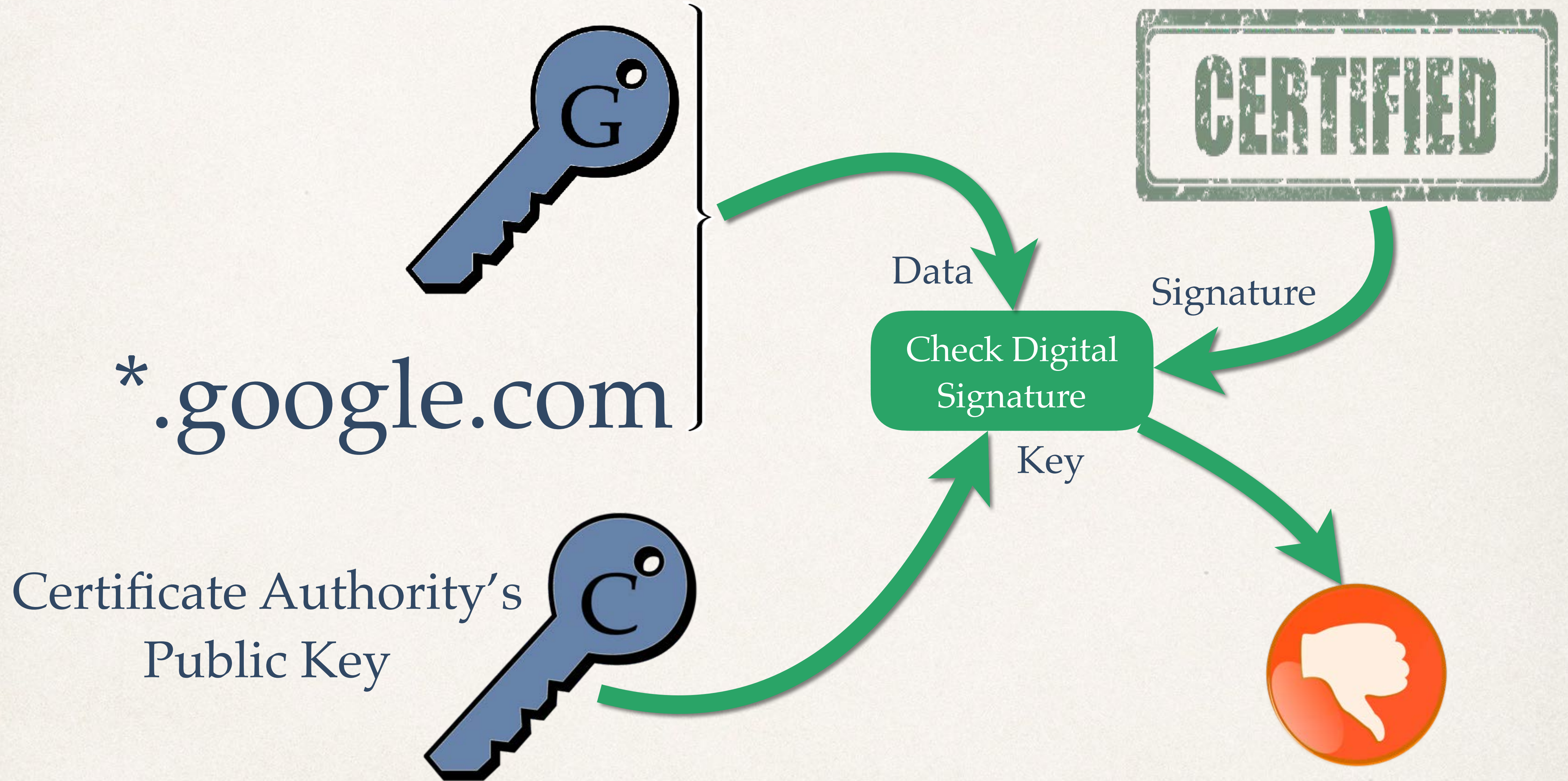
Validating a Certificate



Validating a Certificate



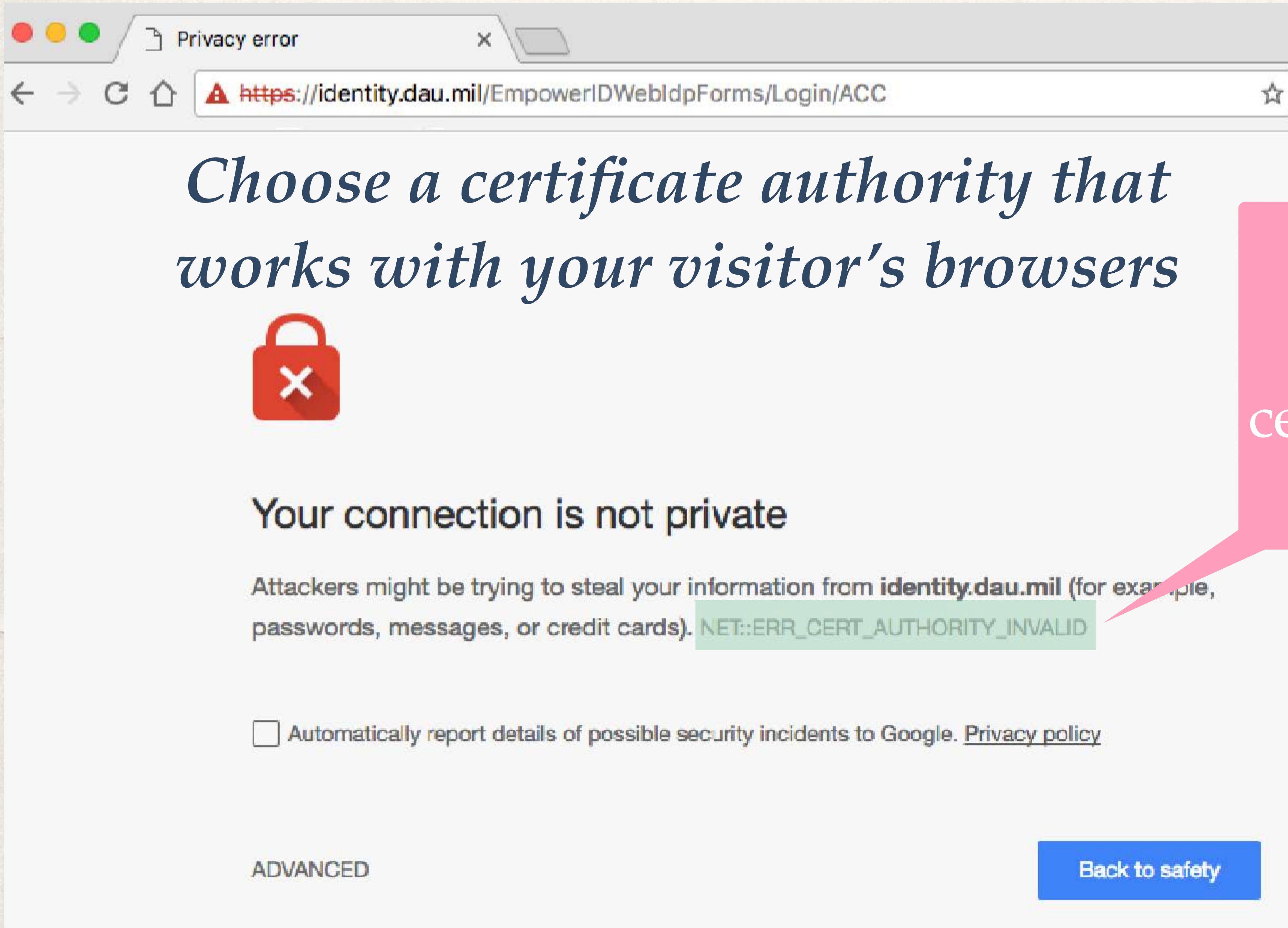
Validating a Certificate



Certificate Authority Failures

<u>Date</u>	<u>Authority</u>	<u>Target Sites</u>	<u>Attack</u>
March 2001	<i>Verisign</i>	❖ Microsoft code signing	Proof of concept: ex MS employee showed he could trick the CA
July 2011	<i>DigiNotar</i>	❖ Google, and over 500 others	CA servers breached; certificates used to intercept email by Google users in Iran
July 2014	<i>India CCA</i>	❖ Google, ❖ Yahoo	Bogus certificates were issued and no published explanation

Which Certificate Authority to Use



Choose a certificate authority that works with your visitor's browsers



Your connection is not private

Attackers might be trying to steal your information from **identity.dau.mil** (for example, passwords, messages, or credit cards). **NET::ERR_CERT_AUTHORITY_INVALID**

☐ Automatically report details of possible security incidents to Google. [Privacy policy](#)

ADVANCED

Back to safety

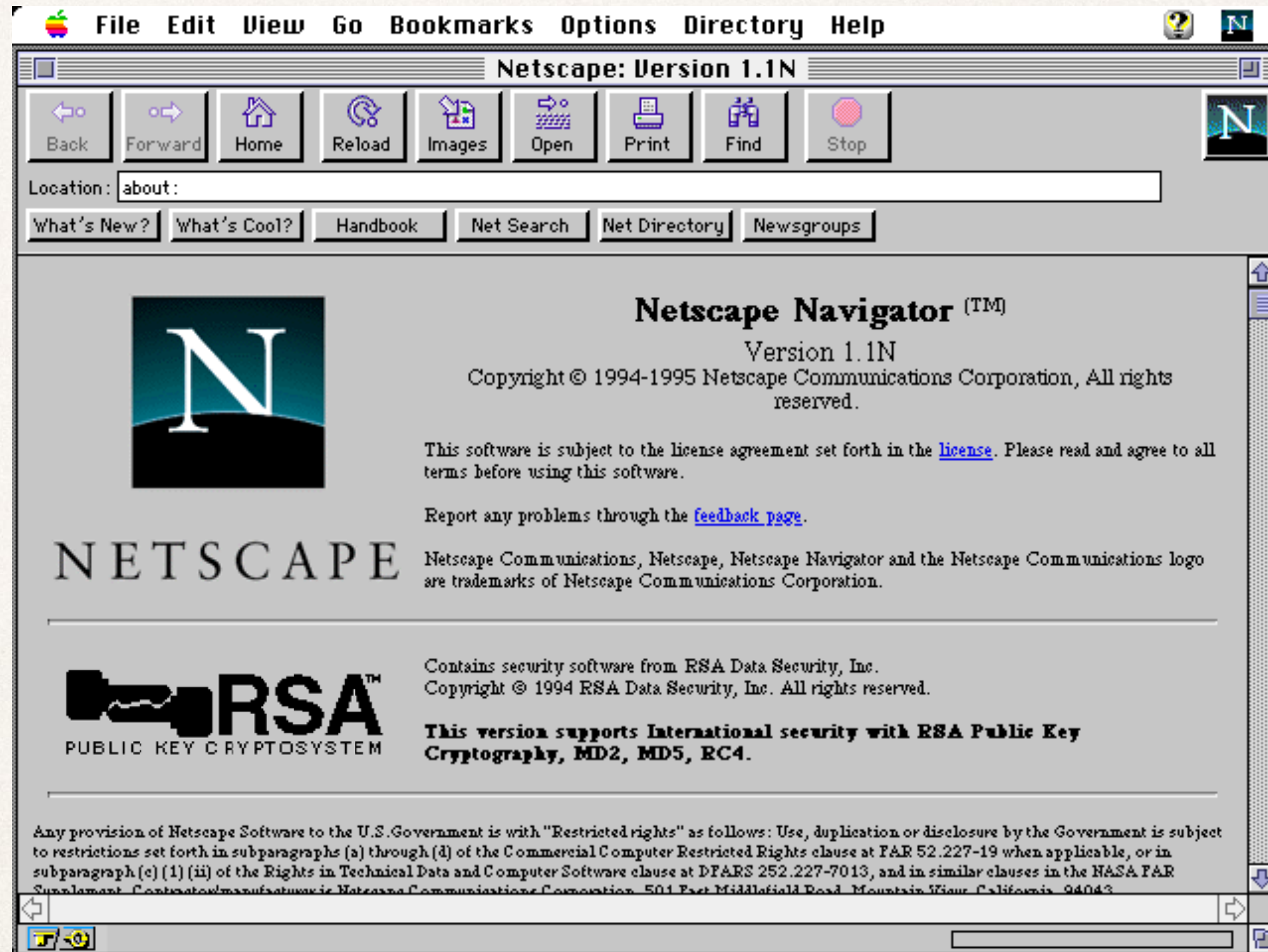
The browser does not know about the certificate authority used by this certificate

Who Signs an SSL/TLS Certificate?

Cryptosmith Video Series #14

Rick Smith, March, 2017

In the Beginning...



The First SSL Certificate Authority



RSA's Certificate
Authority Public Key

RSA's Certificate
Authority Private Key



yahoo.com



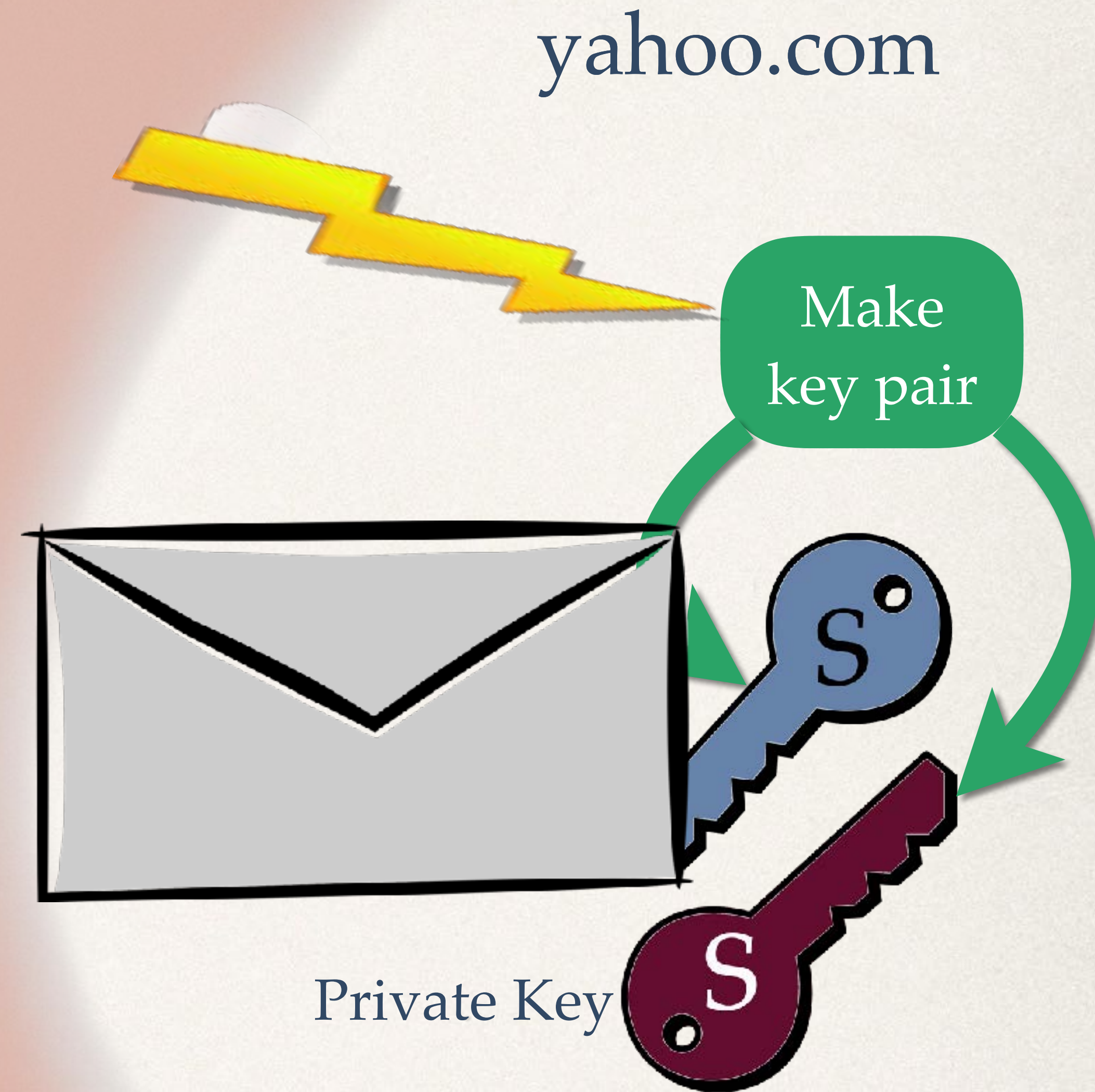
Data

Make Digital
Signature

Key



Issuing a Certificate



Private Key

The Certificate Authority



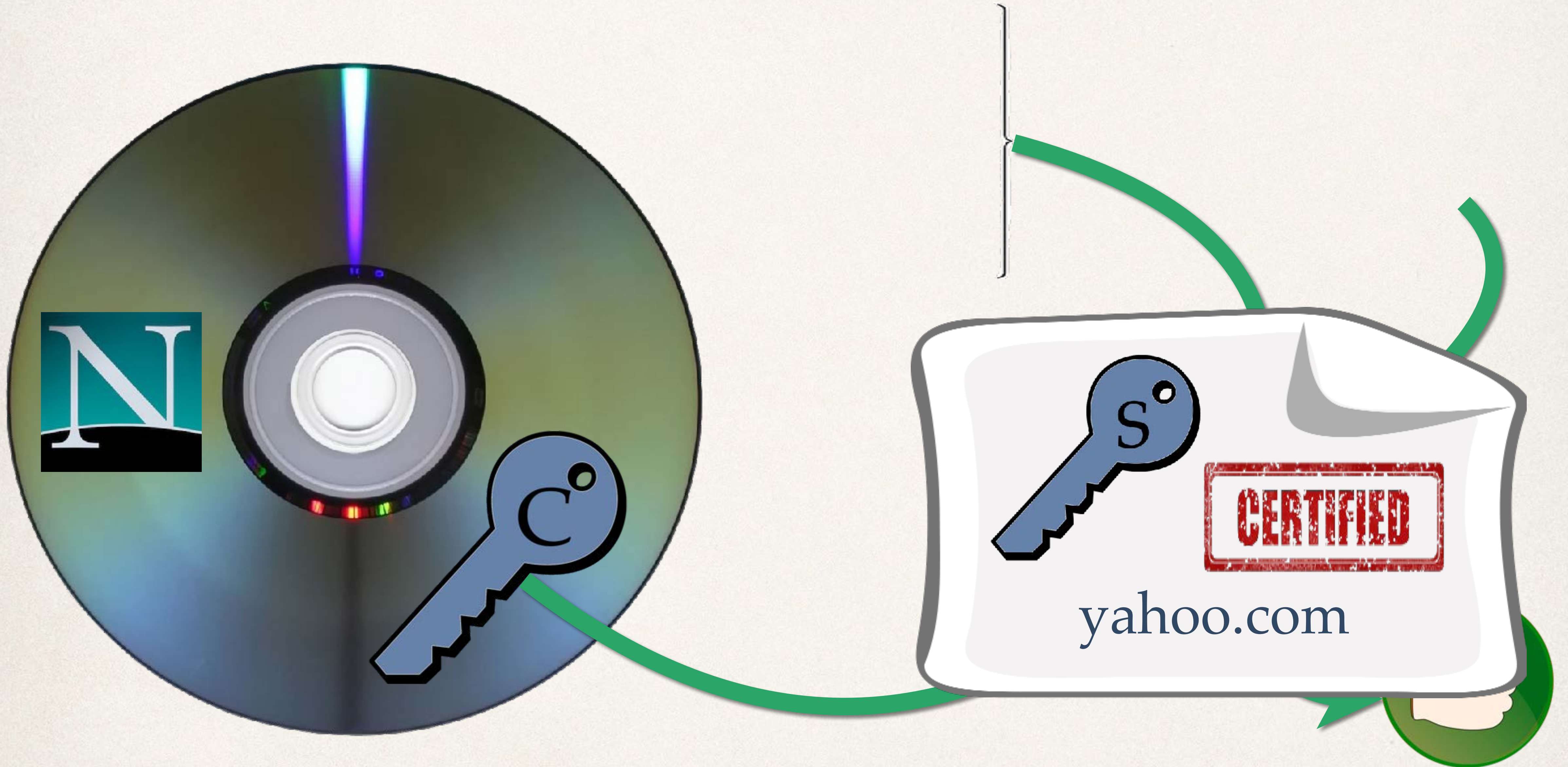
RSA's Certificate
Authority Public Key



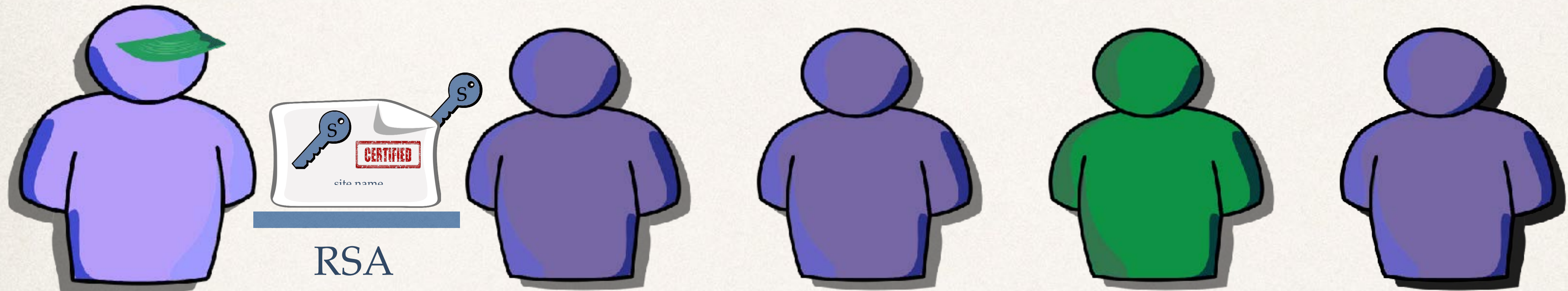
RSA's Certificate
Authority Private Key



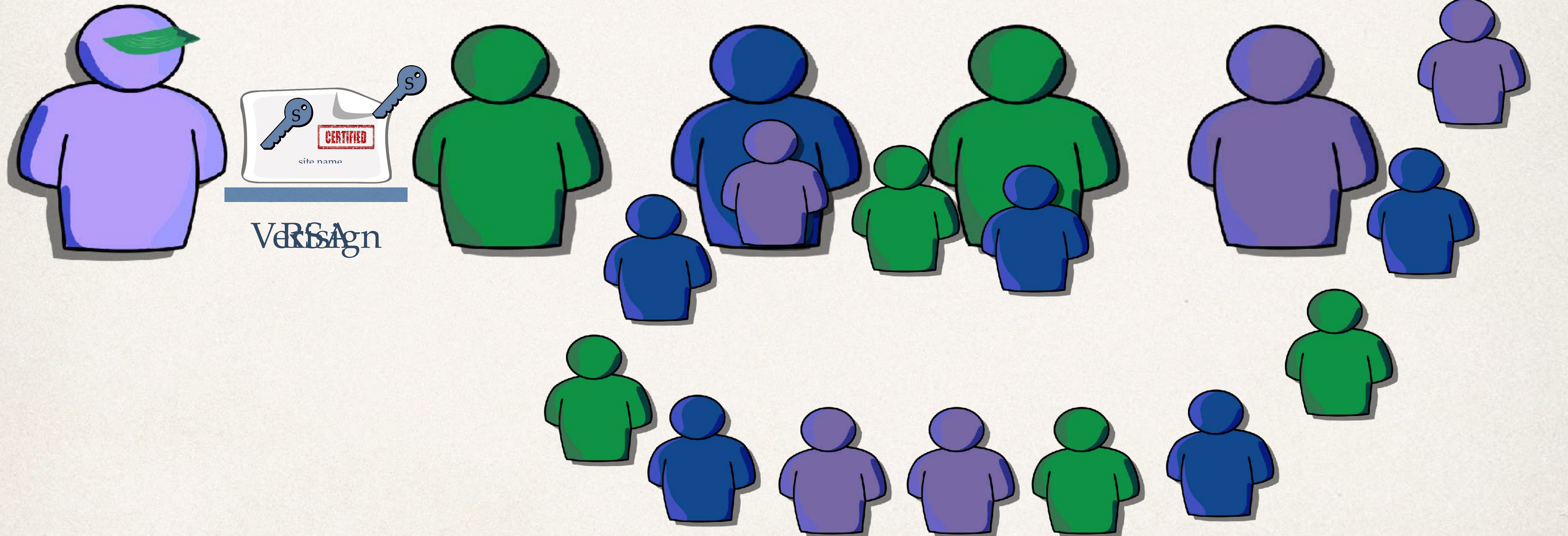
Checking a Certificate



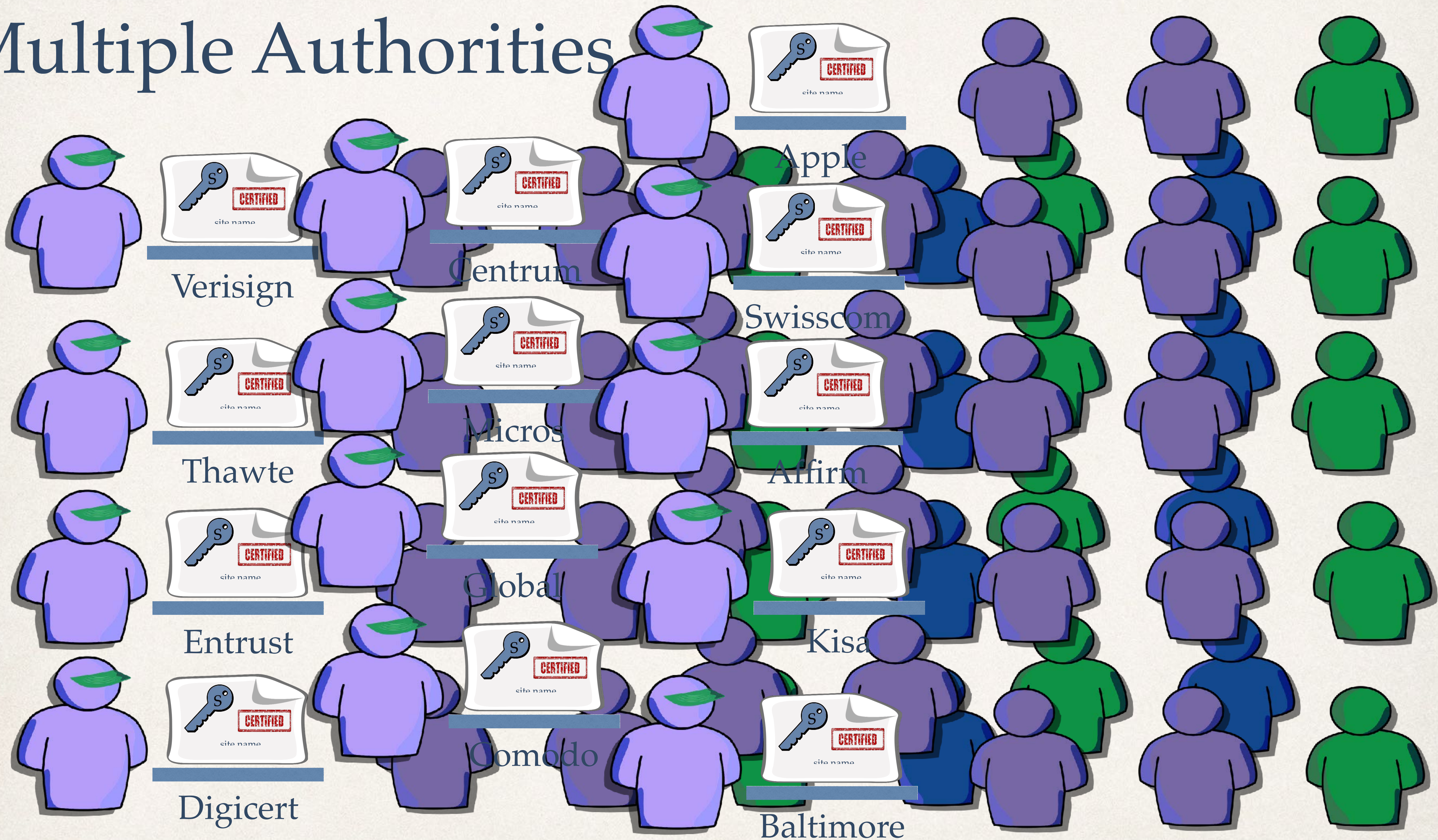
Issuing Certificates by RSA



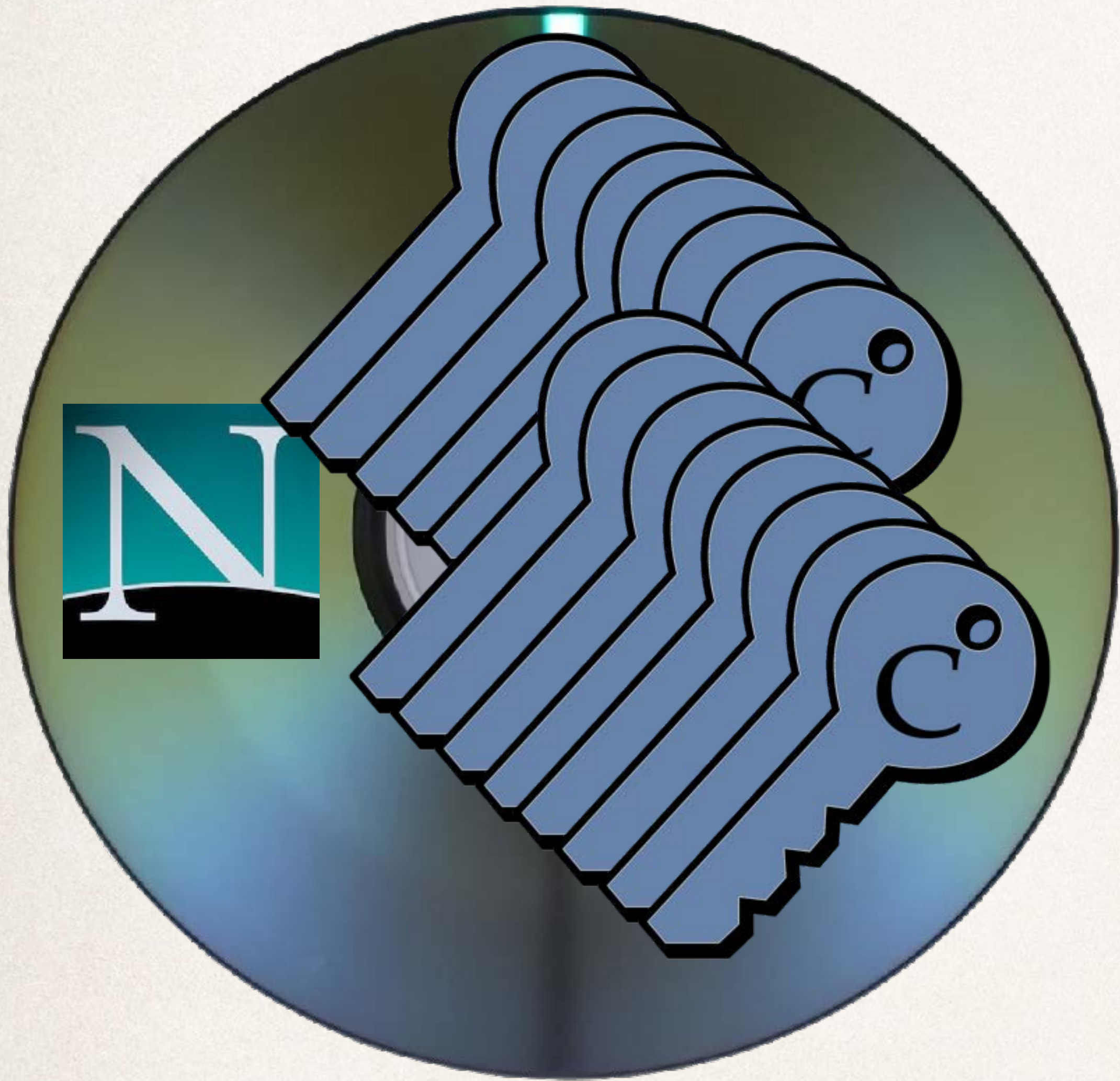
Issuing Certificates by RSA Sign



Multiple Authorities



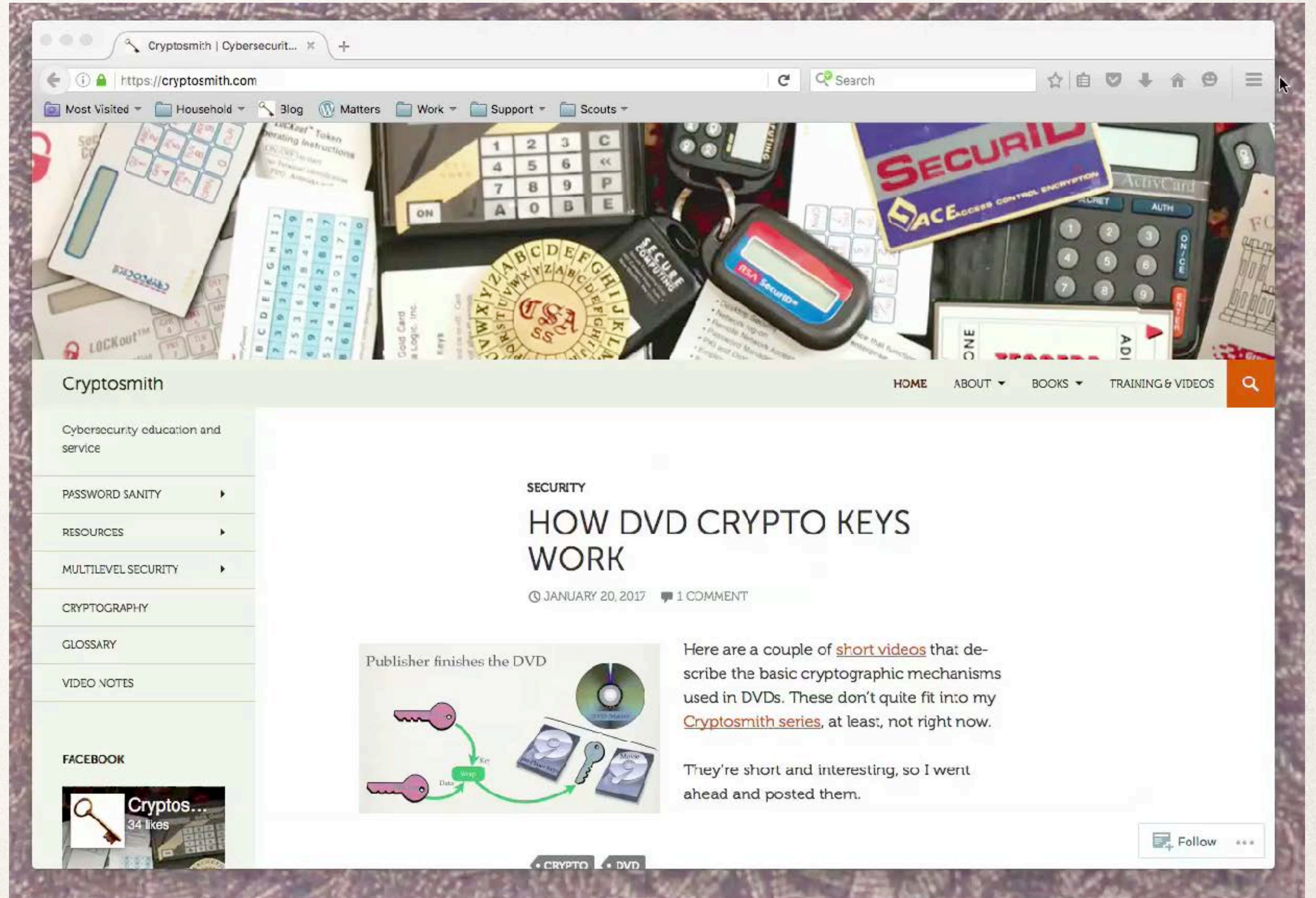
Multiple Authorities



Modern browsers work
with many different
certificate authorities.

Multiple Authorities

Modern browsers keep a list of certificate authorities. Here we retrieve and browse the list in the Firefox browser.



Identifying the Authority



***.google.com**

Issued by: Google Internet Authority G2

Expires: Wednesday, April 26, 2017 at 8:21:00 AM Central Daylight Time

✓ This certificate is valid

▼ Details

Subject Name	
Country	US
State/Province	California
Locality	Mountain View
Organization	Google Inc
Common Name	*.google.com

Certificate
Authority

Checking a Certificate



Checking a Certificate



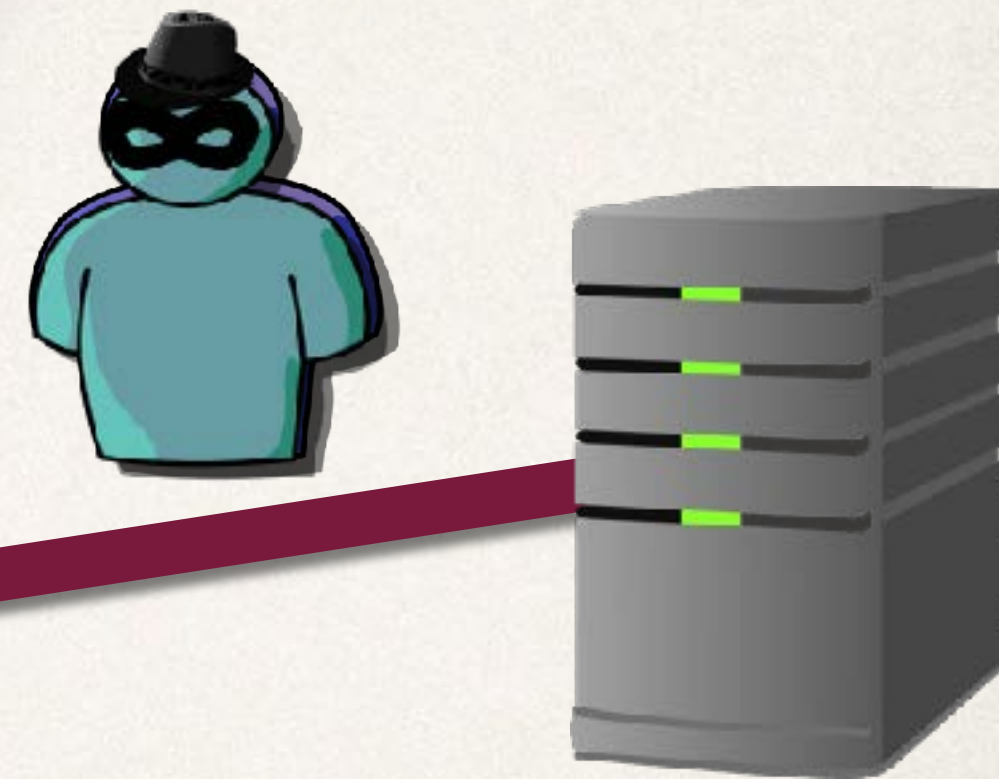
owner: amawig.com

issuer: Let's Encrypt

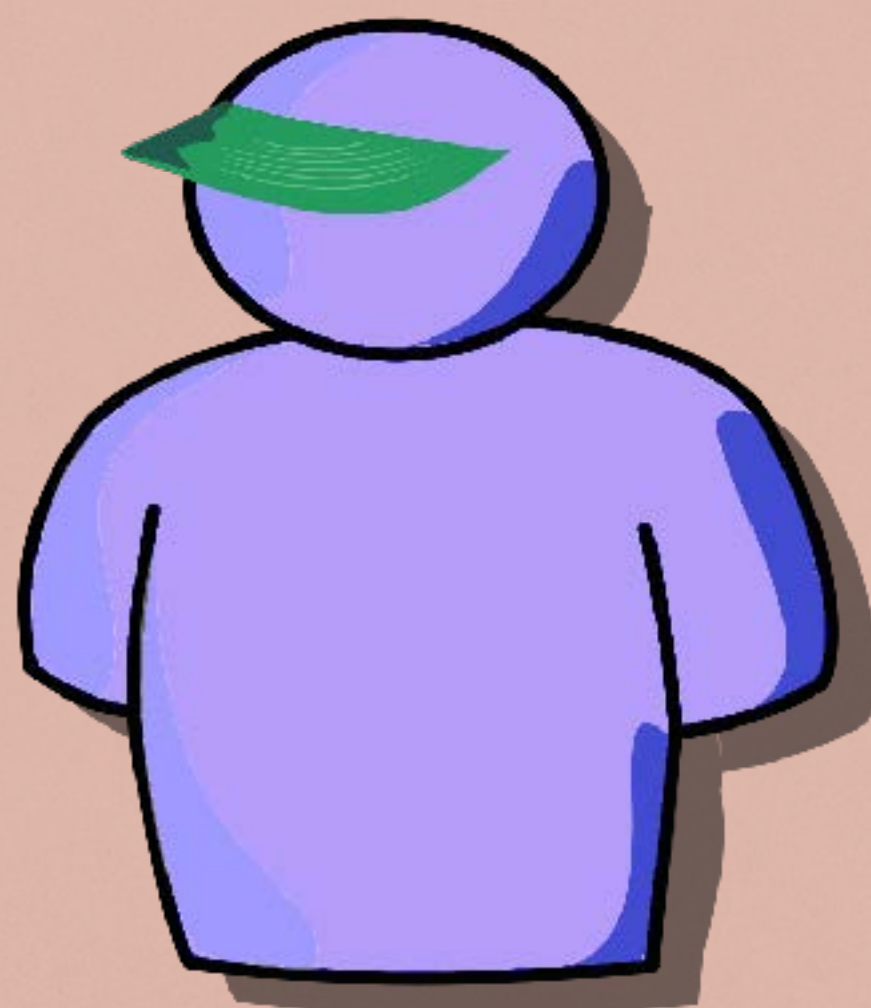
Revoking a Certificate



Revoking a Certificate



<https://www.google.com>



Delegation and Certificate Chains

Cryptosmith Video Series #15

Rick Smith, March, 2017

Validating Google's Certificate



***.google.com**

Issued by: Google Internet Authority G2

Expires: Wednesday, April 26, 2017 at 8:21:00 AM Central Daylight Time

✓ This certificate is valid

▼ Details

Subject Name	
Country	US
State/Province	California
Locality	Mountain View
Organization	Google Inc
Common Name	*.google.com

Certificate
Authority

Validating Google's Certificate

You have certificates on file that identify these certificate authorities:

Certificate Name	Security Device	⌵
Equifax Secure Global eBusiness CA-1	Builtin Object Token	
Equifax Secure eBusiness CA-1	Builtin Object Token	
▼ Generalitat Valenciana		
Root CA Generalitat Valenciana	Builtin Object Token	
▼ GeoTrust Inc.		
GeoTrust Primary Certification Authority - G3	Builtin Object Token	
GeoTrust Primary Certification Authority	Builtin Object Token	
GeoTrust Global CA	Builtin Object Token	
GeoTrust Global CA 2	Builtin Object Token	
GeoTrust Universal CA	Builtin Object Token	
GeoTrust Universal CA 2	Builtin Object Token	
GeoTrust Primary Certification Authority - G2	Builtin Object Token	
GeoTrust SSL CA - G3	Software Security Device	
▼ GlobalSign		
GlobalSign	Builtin Object Token	
GlobalSign	Builtin Object Token	
GlobalSign	Builtin Object Token	
GlobalSign	Builtin Object Token	
▼ GlobalSign nv-sa		
GlobalSign Root CA	Builtin Object Token	
▼ GoDaddy.com, Inc.		
Go Daddy Root Certificate Authority - G2	Builtin Object Token	
Go Daddy Secure Certificate Authority - G2	Software Security Device	
▼ Government Root Certification Authority		
Taiwan GRCA	Builtin Object Token	
▼ Hellenic Academic and Research Institutions Cert. Authority		
Hellenic Academic and Research Institutions RootCA 2011	Builtin Object Token	

Validating Google's

Alphabetical Listing

GoDaddy

Google G2

Government

?

- GeoTrust Universal CA 2
- GeoTrust Primary Certification Authority - G2
- GeoTrust SSL CA - G3
- ▼ GlobalSign
 - GlobalSign
 - GlobalSign
 - GlobalSign
 - GlobalSign
- ▼ GlobalSign nv-sa
 - GlobalSign Root CA
- ▼ GoDaddy.com, Inc.
 - Go Daddy Root Certificate Authority - G2
 - Go Daddy Secure Certificate Authority - G2
- ▼ Government Root Certification Authority
 - Taiwan GRCA
- ▼ Hellenic Academic and Research Institutions Cert. Authority
 - Hellenic Academic and Research Institutions RootCA 201

Authority G2's Certificate



Google Internet Authority G2

Intermediate certificate authority

Expires: Sunday, December 31, 2017 at 5:59:59 PM Central Standard Time

✓ This certificate is valid

▼ Details

Subject Name	
Country	US
Organization	Google Inc
Common Name	Google Internet Authority G2



Intermediate certificate authority

Expires: Sunday, December 31, 2017 at 5:59:59 PM Central Standard Time

✓ This certificate is valid

▼ **Details**

Subject Name

Country US

Organization Google Inc

Common Name Google Internet Authority G2

Issuer Name

Country US

Organization GeoTrust Inc.

Common Name GeoTrust Global CA

One Certificate Validates Another



www.google.com

Issued by: Google Internet Authority G2

Expires: Wednesday, May 31, 2017 at 9:19:00 PM Central Daylight Time

✓ This certificate is valid

▼ Details

Subject Name
Country U
State/Province C
Locality M
Organization G
Common Name w



Google Internet Authority G2

Intermediate certificate authority

Expires: Sunday, December 31, 2017 at
Standard Time

✓ This certificate is valid

▼ Details

Subject Name
Country US
Organization Google Inc
Common Name Google Internet Authority G2

Issuer Name
Country US
Organization GeoTrust Inc.
Common Name GeoTrust Global CA



GeoTrust Global CA

Root certificate authority

Expires: Friday, May 20, 2022 at 11:00:00 PM Central Daylight Time

✓ This certificate is valid

▼ Details

Subject Name
Country US
Organization GeoTrust Inc.
Common Name GeoTrust Global CA

Issuer Name
Country US
Organization GeoTrust Inc.
Common Name GeoTrust Global CA


Sharing Intermediate Certificates





<https://www.google.com>




A Certificate Chain

 **GeoTrust Global CA**

↳  **Google Internet Authority G2**

↳  ***.google.com**



GeoTrust Global CA


Root certificate authority


Expires: Friday, May 20, 2022 at 11:00:00 PM Central Daylight Time


✔ This certificate is valid


▶ **Details**

A Certificate Chain

 GeoTrust Global CA

 Google Internet Authority G2

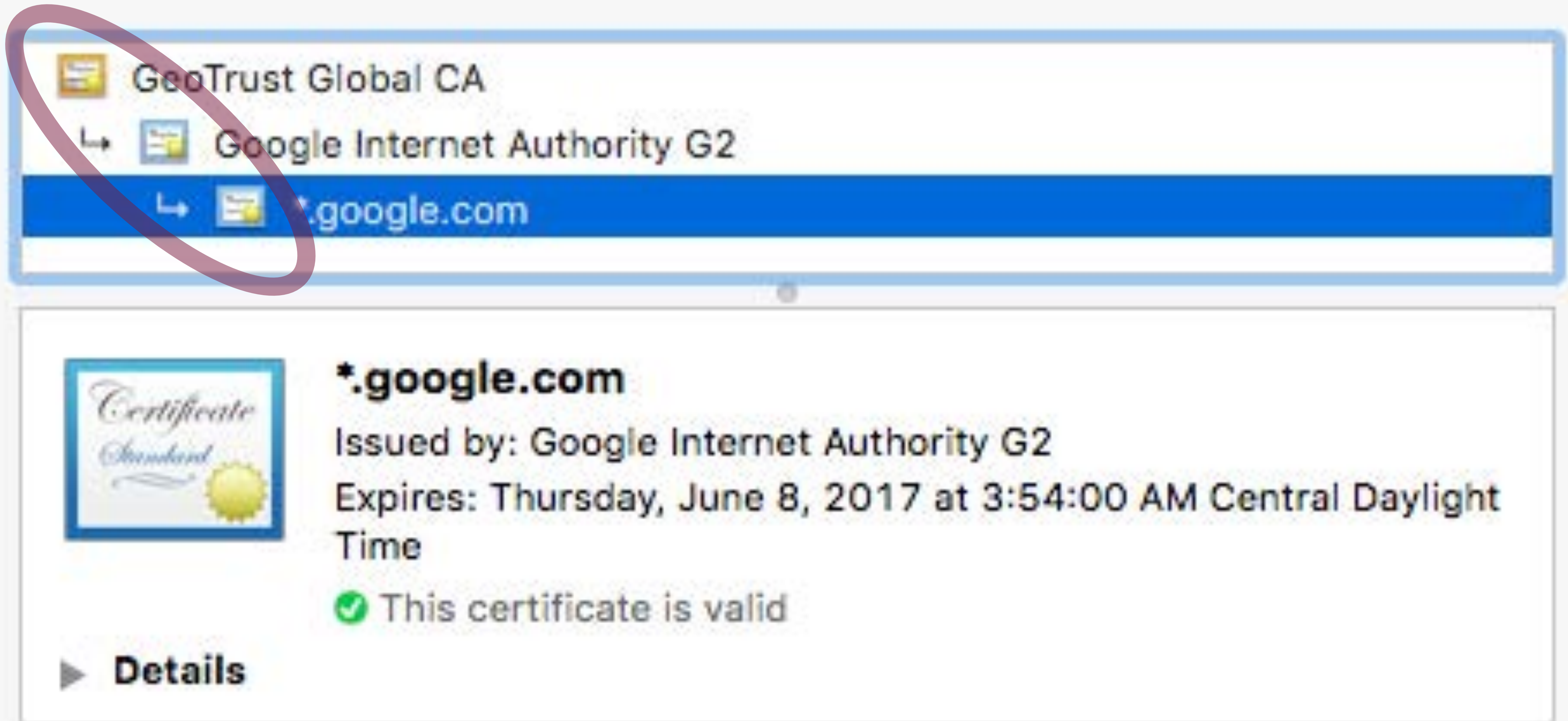
 *.google.com



Google Internet Authority G2
Intermediate certificate authority
Expires: Sunday, December 31, 2017 at 5:59:59 PM Central Standard Time
✔ This certificate is valid

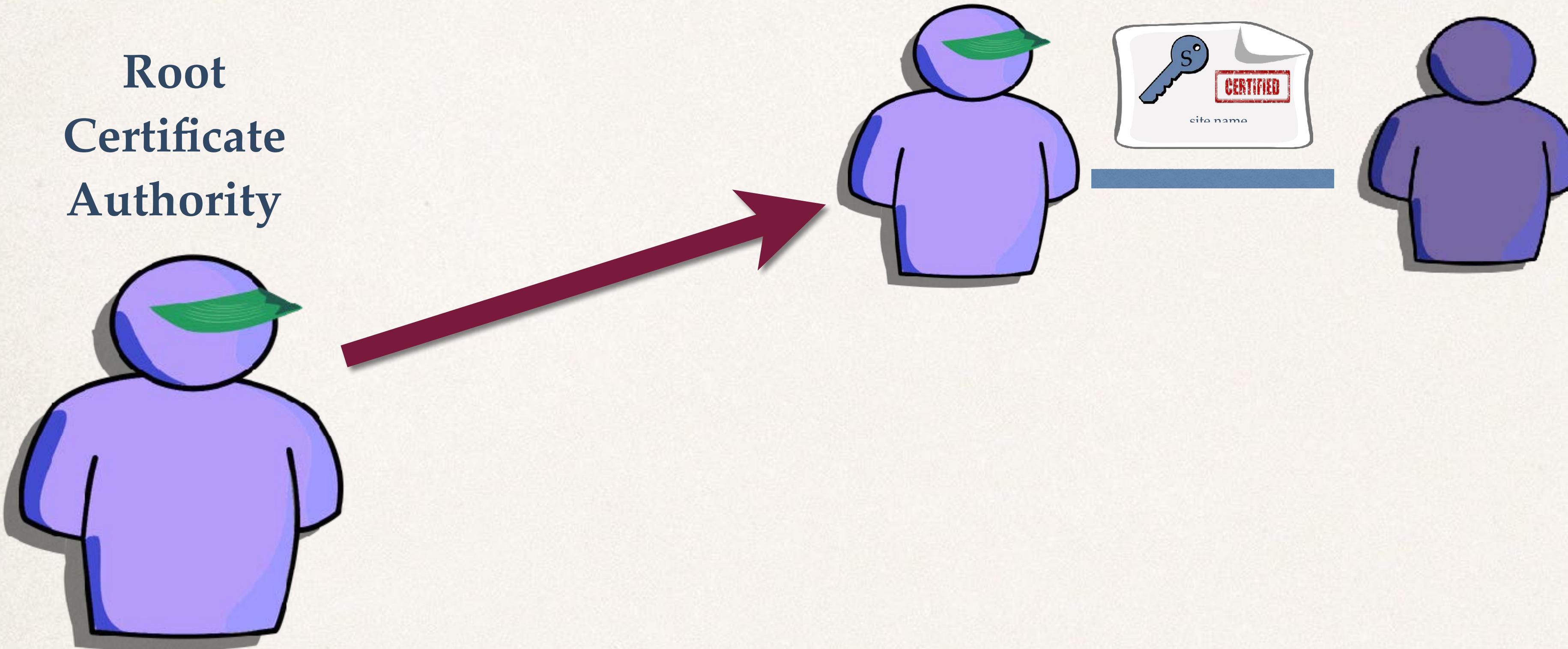
► **Details**

A Certificate Chain



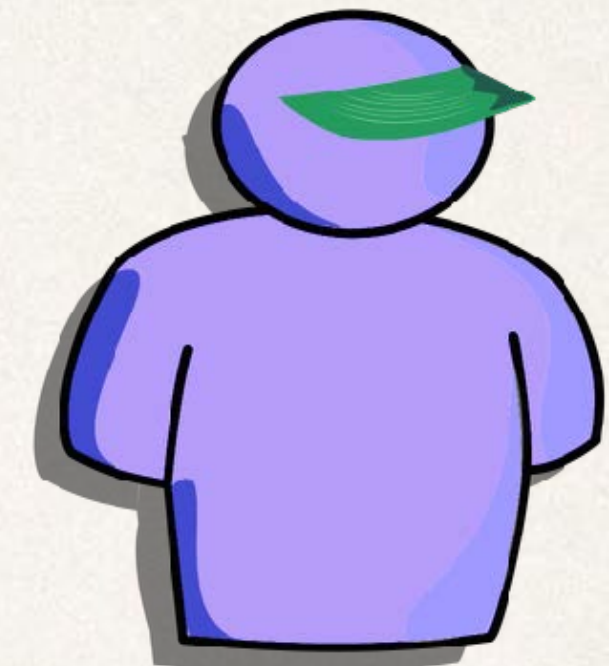
Delegation

Root
Certificate
Authority

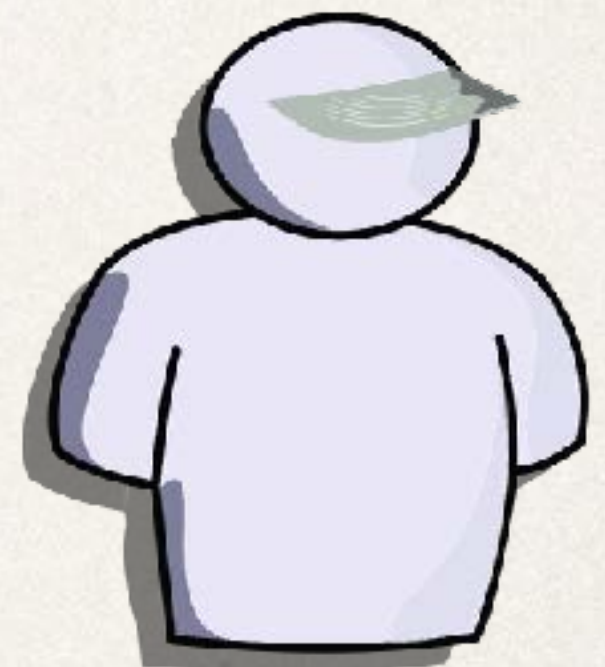
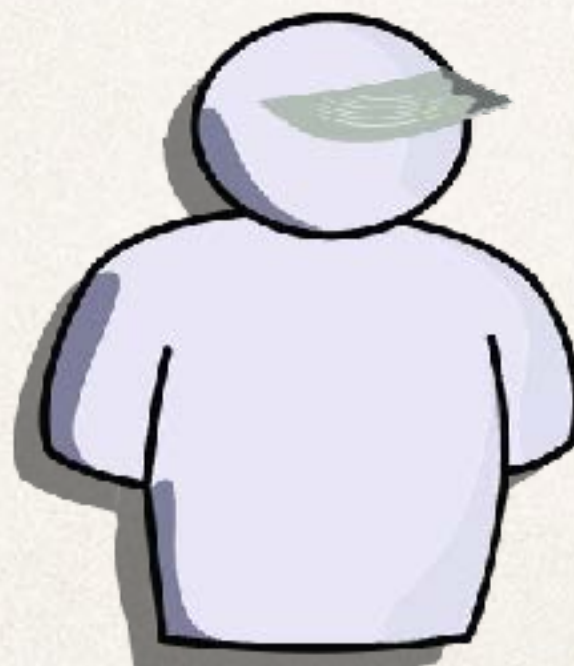
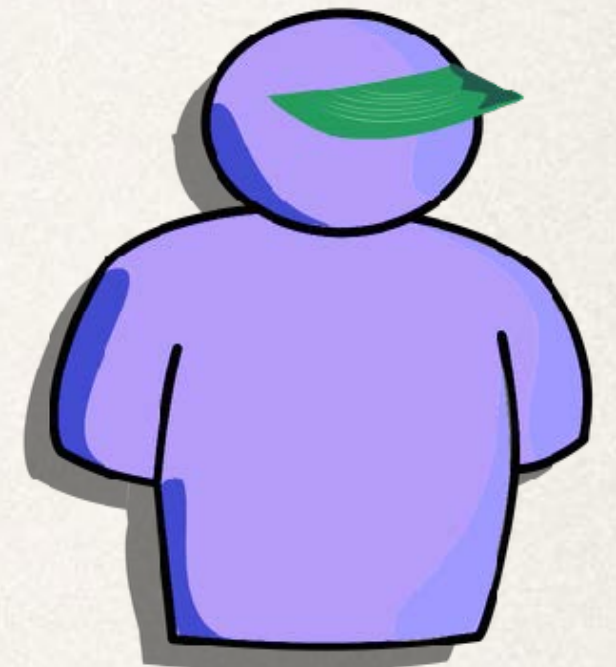


Delegation

Root
Certificate
Authority



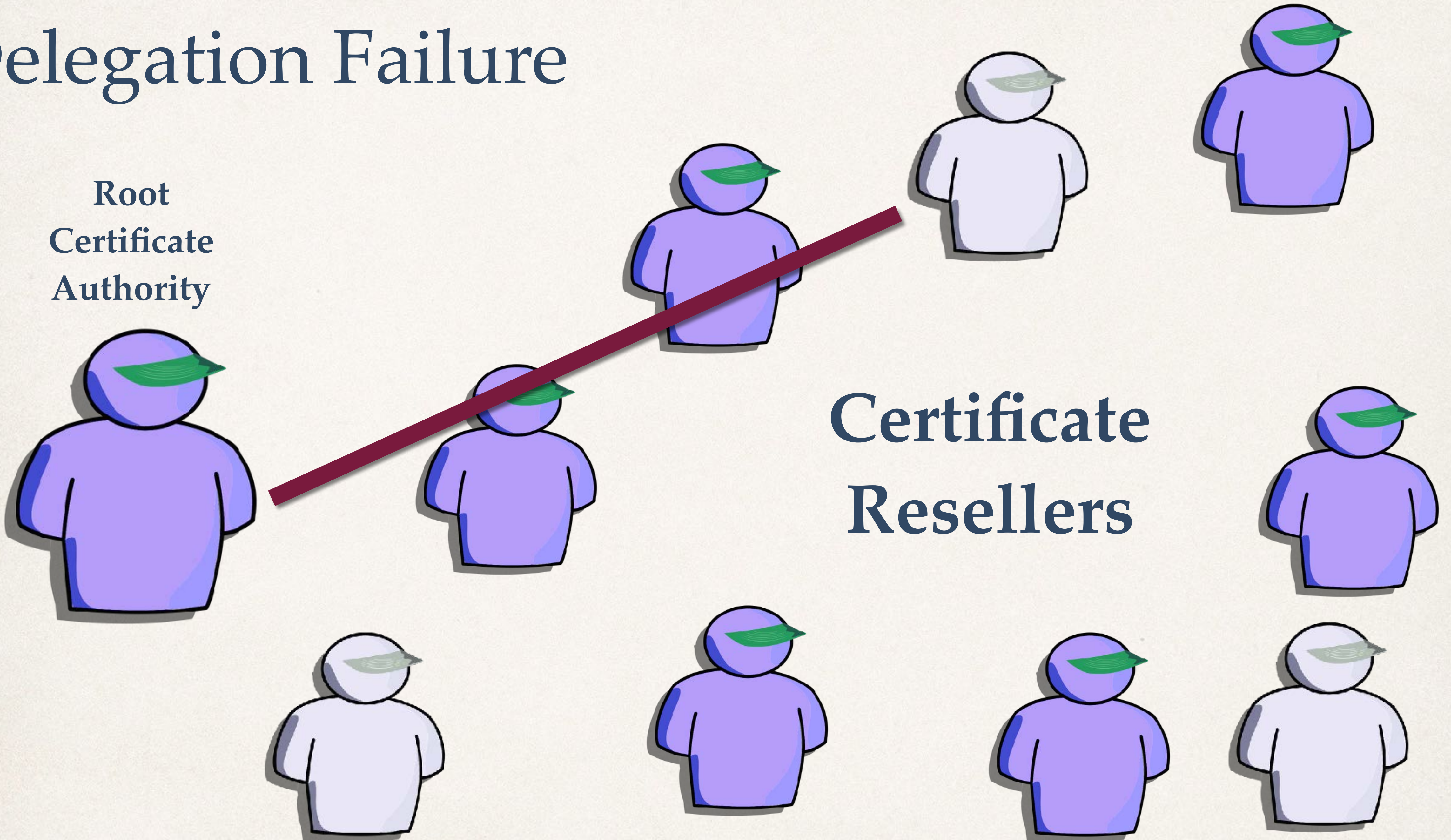
Certificate
Resellers



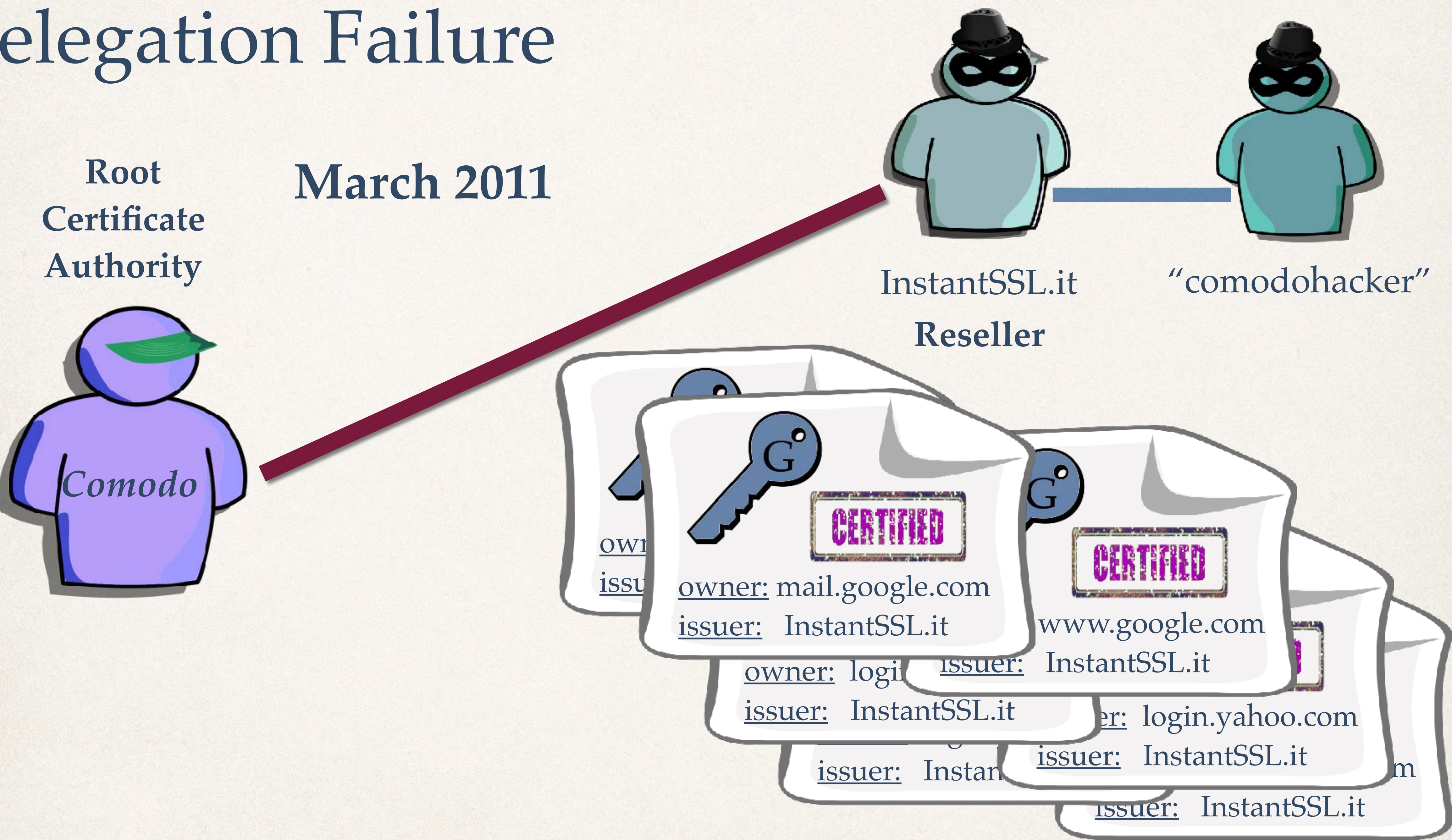
Delegation Failure

Root
Certificate
Authority

Certificate
Resellers



Delegation Failure



How do we distribute
public keys?

Certificates

How do we sign
certificates?

Certificate Authorities

How do we verify
certificate signatures?

Root Certificates

How do we get root
certificates?

Browser Software

Public
Key
Infrastructure

(PKI)



Copyright 2017 Cryptosmith Institute