

Criptografía: Firma Digital y Certificados Digitales



AGENDA

- Firmas
- Firma Digital Clave Privada
- Firma Digital Clave Pública
- Función Resumen
- Certificados Digitales

OBJETIVOS DE LA CRIPTOGRAFÍA

- ¿Qué problemas quiero resolver?
 - **Confidencialidad:** Garantizar que el mensaje solo pueda ser leído por los autorizados
 - **Autenticación:** Identificar una característica de un objeto. En general, asegurarse que una persona es quien dice ser
 - **Integridad:** Asegurarse que el mensaje no fue modificado de forma no autorizada
 - **No repudio:** Evitar que alguien rechace ser autor de algo



FIRMA

¿Qué problemas resuelve la firma (holográfica) de un documento?

- Autenticación
- No repudio

Procedimiento de Firma

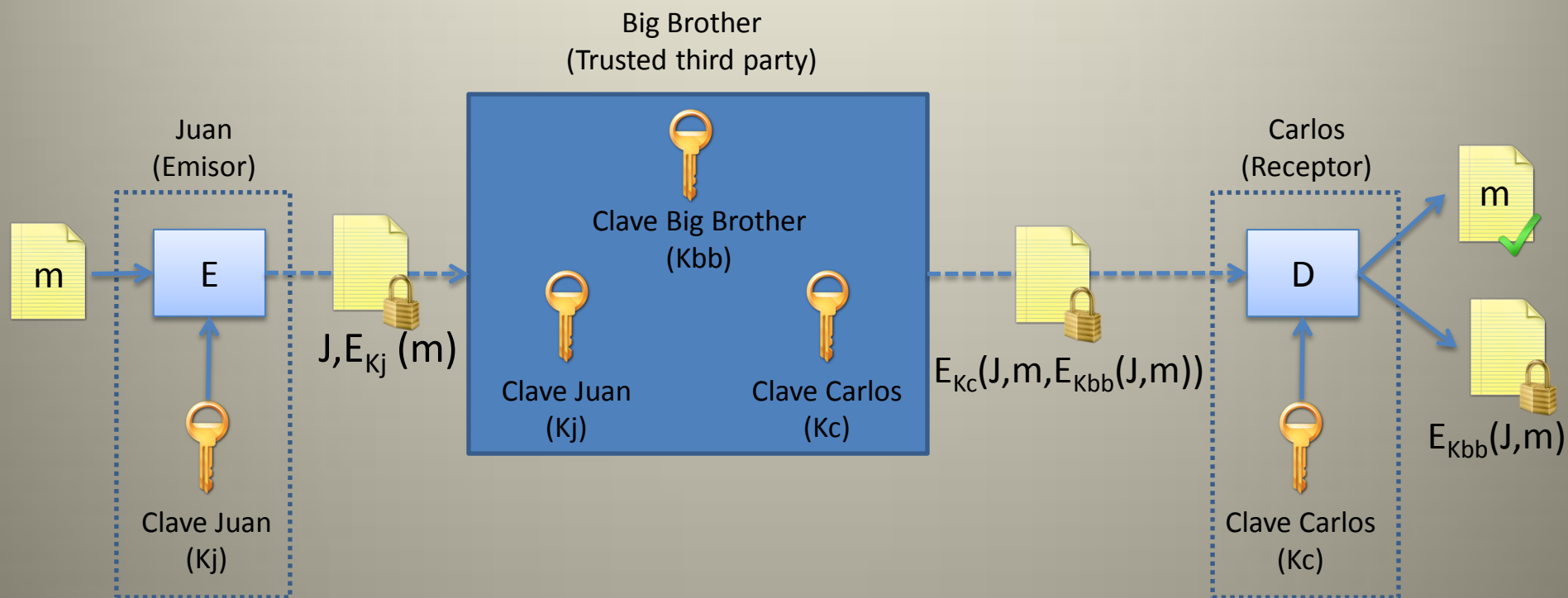
- Asiento de la Firma en un Documento
- Proceso de Firma
- Proceso de Verificación

¿Cómo puedo lograr que esto pueda ser realizado entre dos computadoras?

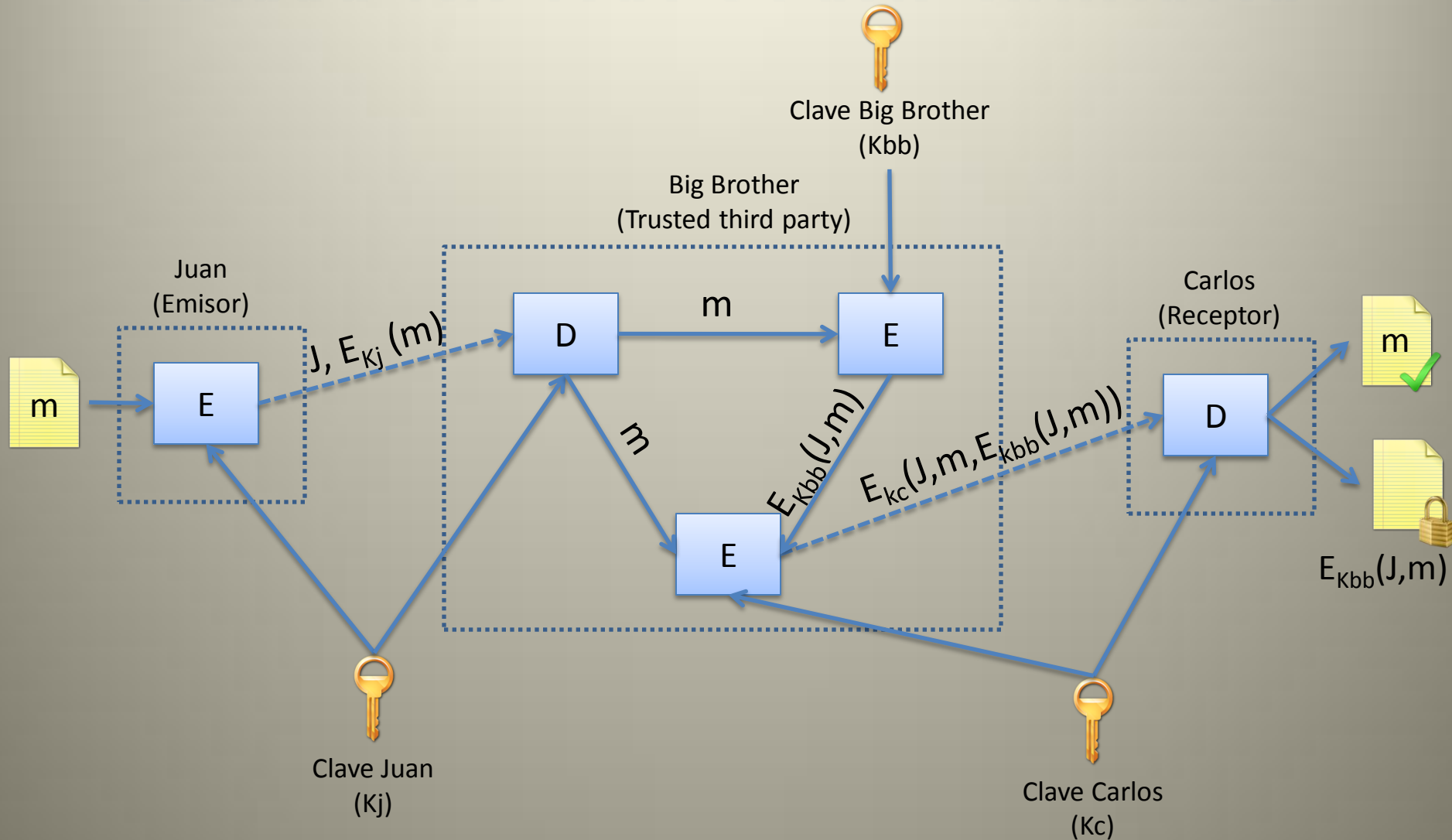


FIRMA DIGITAL CLAVE PRIVADA

- Se basa en la criptografía **simétrica**
- Provee confidencialidad, autenticación y no repudio



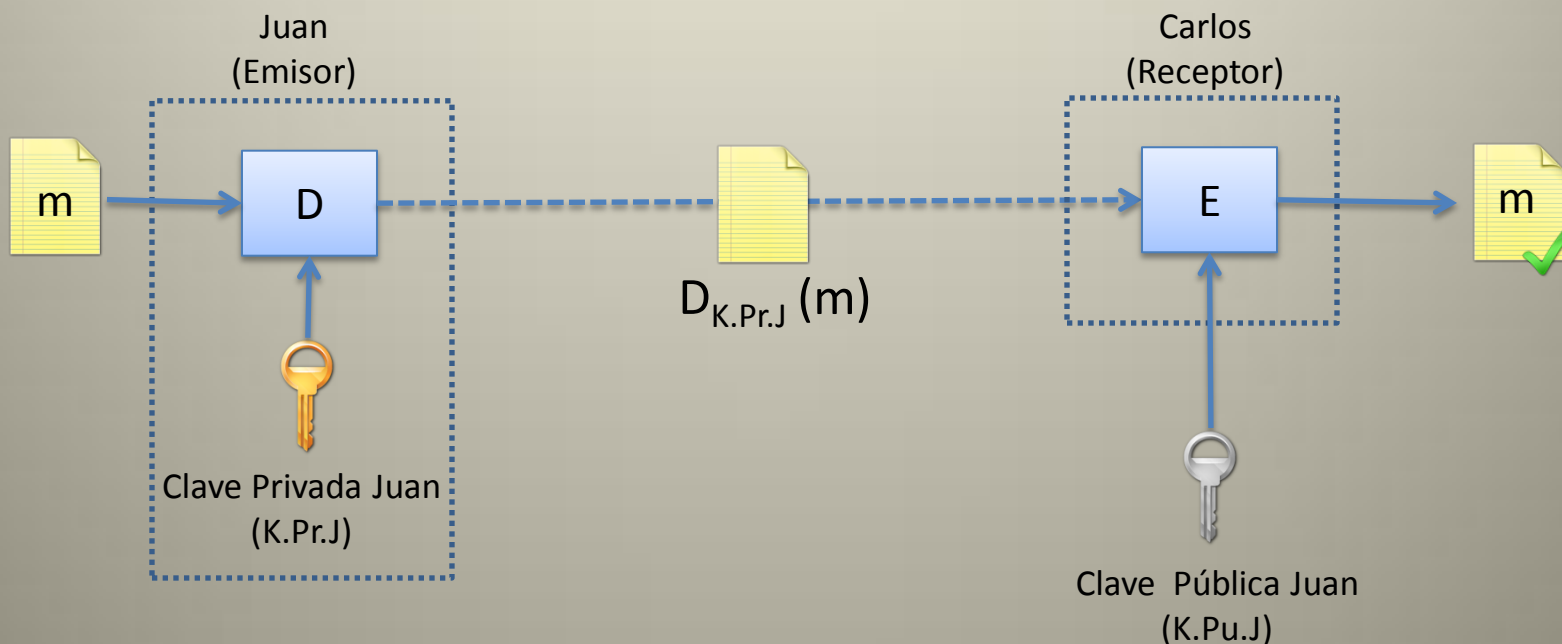
FIRMA DIGITAL CLAVE PRIVADA





FIRMA DIGITAL CLAVE PÚBLICA

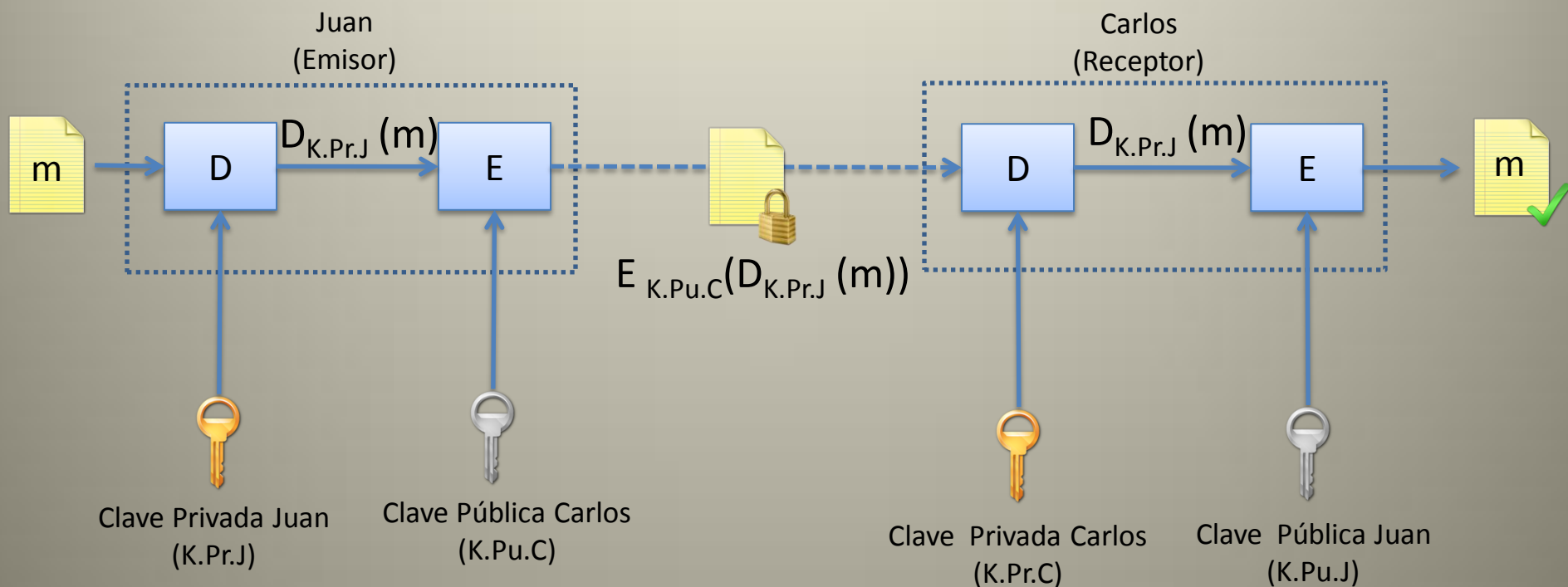
- Se basa en la criptografía **asimétrica**
- Provee autenticación y no repudio (*)





FIRMA DIGITAL CLAVE PÚBLICA

- Provee autenticación, no repudio y confidencialidad (*)



FUNCIÓN RESUMEN

- ¿Cómo lograr integridad? ¿Cómo acelerar el proceso firma?

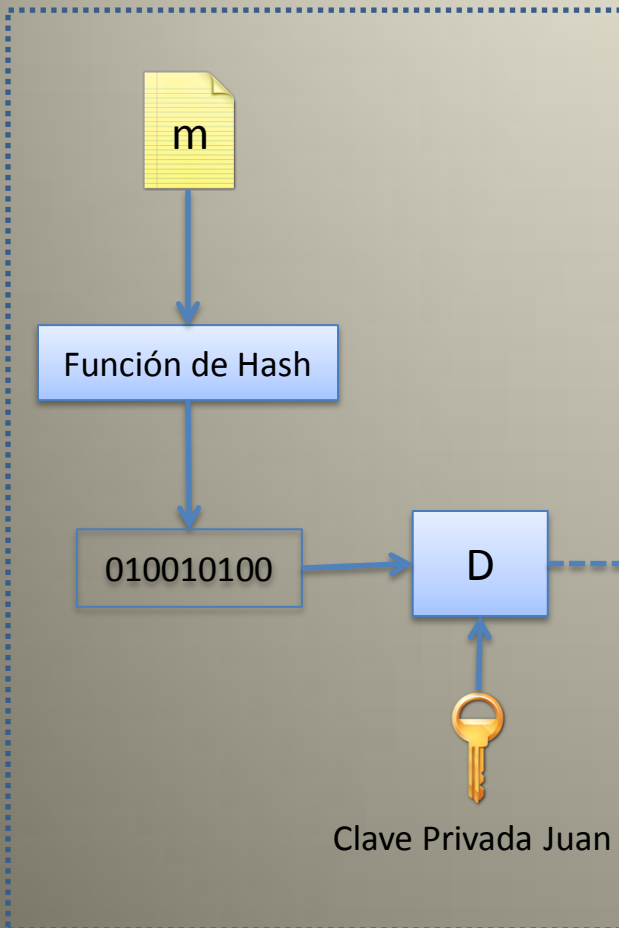


- La función tiene las siguientes **características**:
 - Dado m , es fácil calcular $r(m)$
 - Dado $r(m)$, es imposible calcular m
 - Dado m , no se puede encontrar m' de manera tal que $r(m') = r(m)$
 - Un cambio de m de incluso un bit produce una salida muy diferente

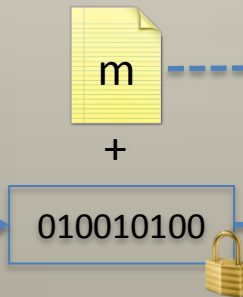
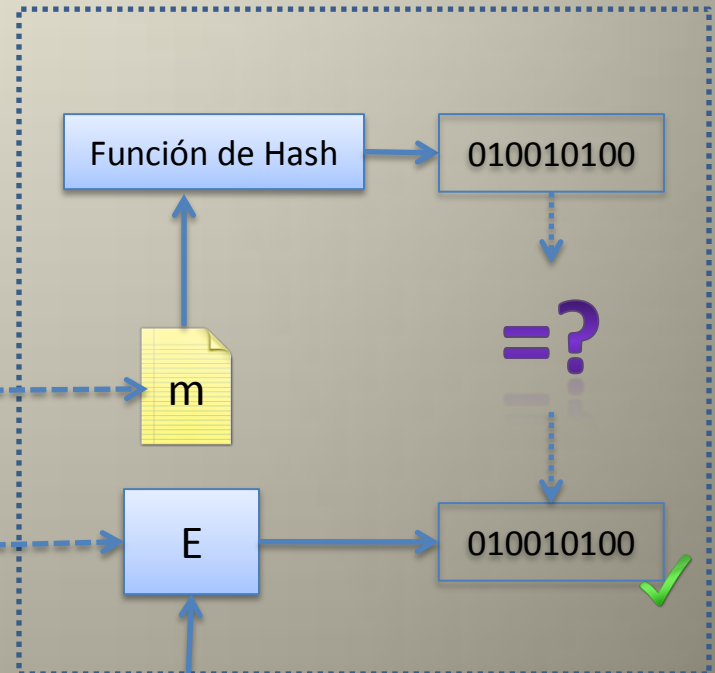
FIRMA DIGITAL CON RESUMEN

- Función resumen aplicada a un esquema asimétrico. Provee autenticación, no repudio e integridad

Juan
(Emisor)



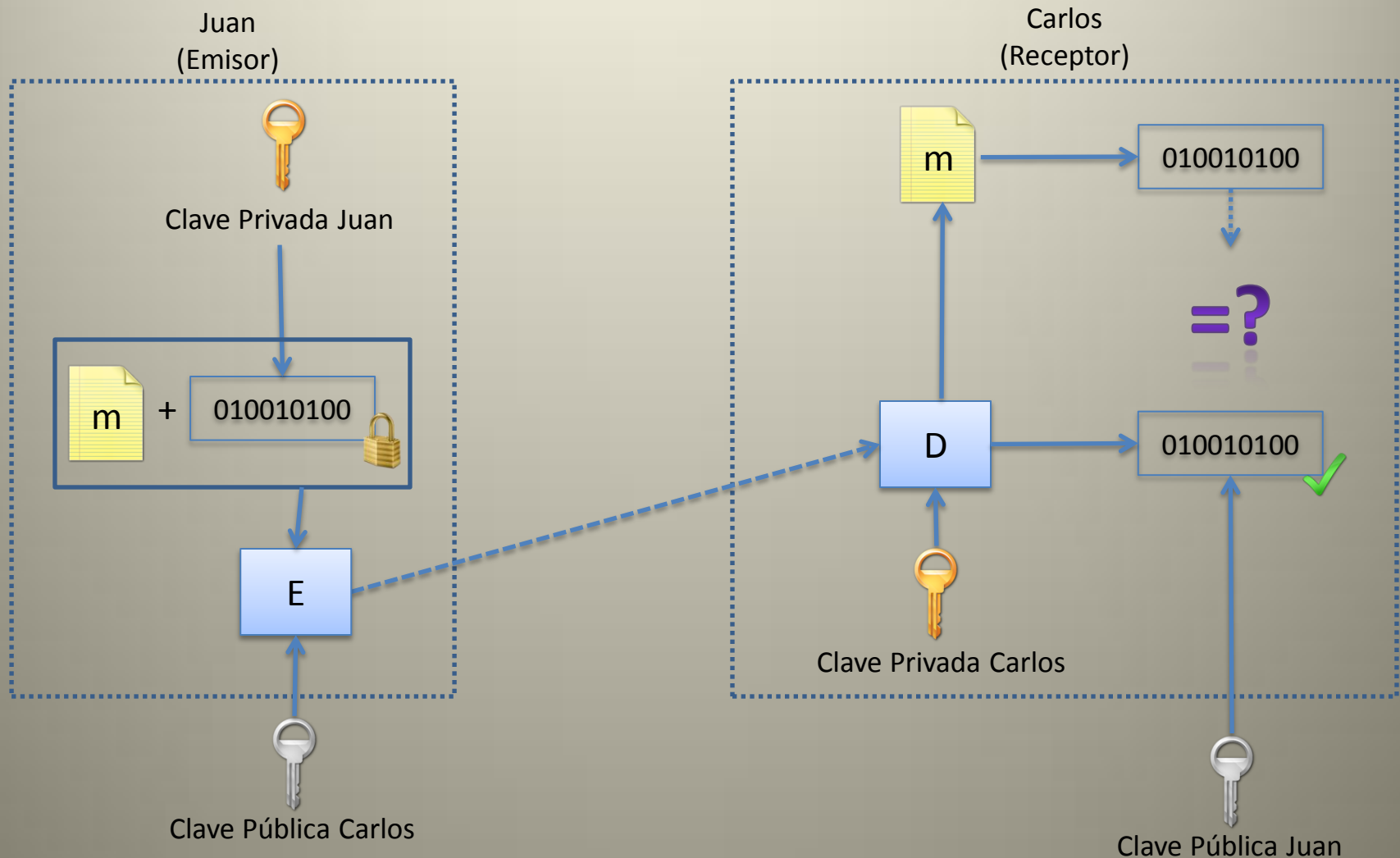
Carlos
(Receptor)



Clave Pública Juan

FIRMA DIGITAL CON RESUMEN

- Proveyendo autenticación, no repudio, integridad y confidencialidad





CERTIFICADOS DIGITALES

• ¿Cómo obtener de forma segura la clave pública de otra persona?

✗ Centro de distribución de claves públicas

✓ Autoridad certificante + certificado digital de claves públicas

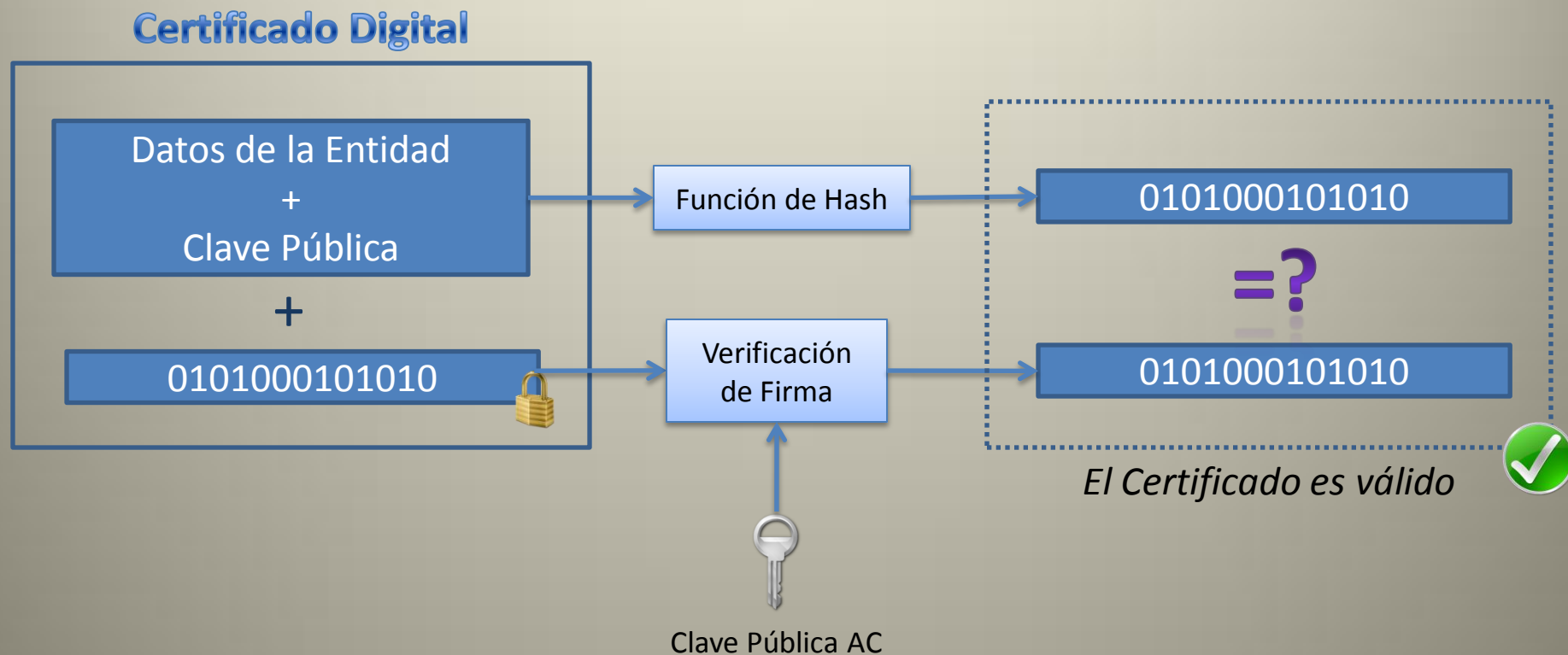


El objetivo de un certificado digital es relacionar inequívocamente una persona con su clave pública. (*) Si la clave no estuviese certificada, no podría asegurar autenticación o no repudio, a menos que hubiesen sido intercambiadas personalmente.



CERTIFICADOS DIGITALES

•Proceso de verificación del certificado digital



La seguridad del sistema de certificados digitales reside en la seguridad de la clave privada de la AC.



CERTIFICADOS DIGITALES

- Ejemplo de un certificado digital real



Información del certificado

Este certificado está destinado a los siguientes propósitos:

- Asegura la identidad de un equipo remoto

Emitido por: mail.google.com

Emitido por: Thawte SGC CA

Válido desde: 25/03/2009 **hasta:** 25/03/2010

Campo	Valor
Número de serie	6e df 0d 94 99 fd 45 33 dd 12 ...
Algoritmo de firma	sha1RSA
Emisor	Thawte SGC CA, Thawte Cons...
Válido desde	miércoles, 25 de marzo de 200...
Válido hasta	jueves, 25 de marzo de 2010 ...
Asunto	mail.google.com, Google Inc, ...
Clave pública	RSA (1024 Bits)
Uso mejorado de claves	Autenticación del servidor (1, 3)

30	81	89	02	81	81	00	c5	d6	f8	92	fc	ca	f5
61	4b	06	41	49	e8	0a	2c	95	81	a2	18	ef	41
ec	35	bd	7a	58	12	5a	e7	6f	9e	a5	4d	dc	89
3a	bb	eb	02	9f	6b	73	61	6b	f0	ff	d8	68	79
1f	ba	7a	f9	c4	ae	bf	37	06	ba	3e	ea	ee	d2
74	35	b4	dd	cf	b1	57	c0	5f	35	1d	66	aa	87
fe	e0	de	07	2d	66	d7	73	af	fb	d3	6a	b7	8b
ef	09	0e	0c	c8	61	a9	03	ac	90	dd	98	b5	1c
9c	41	56	6c	01	7f	0b	ee	c3	bf	f3	91	05	1f