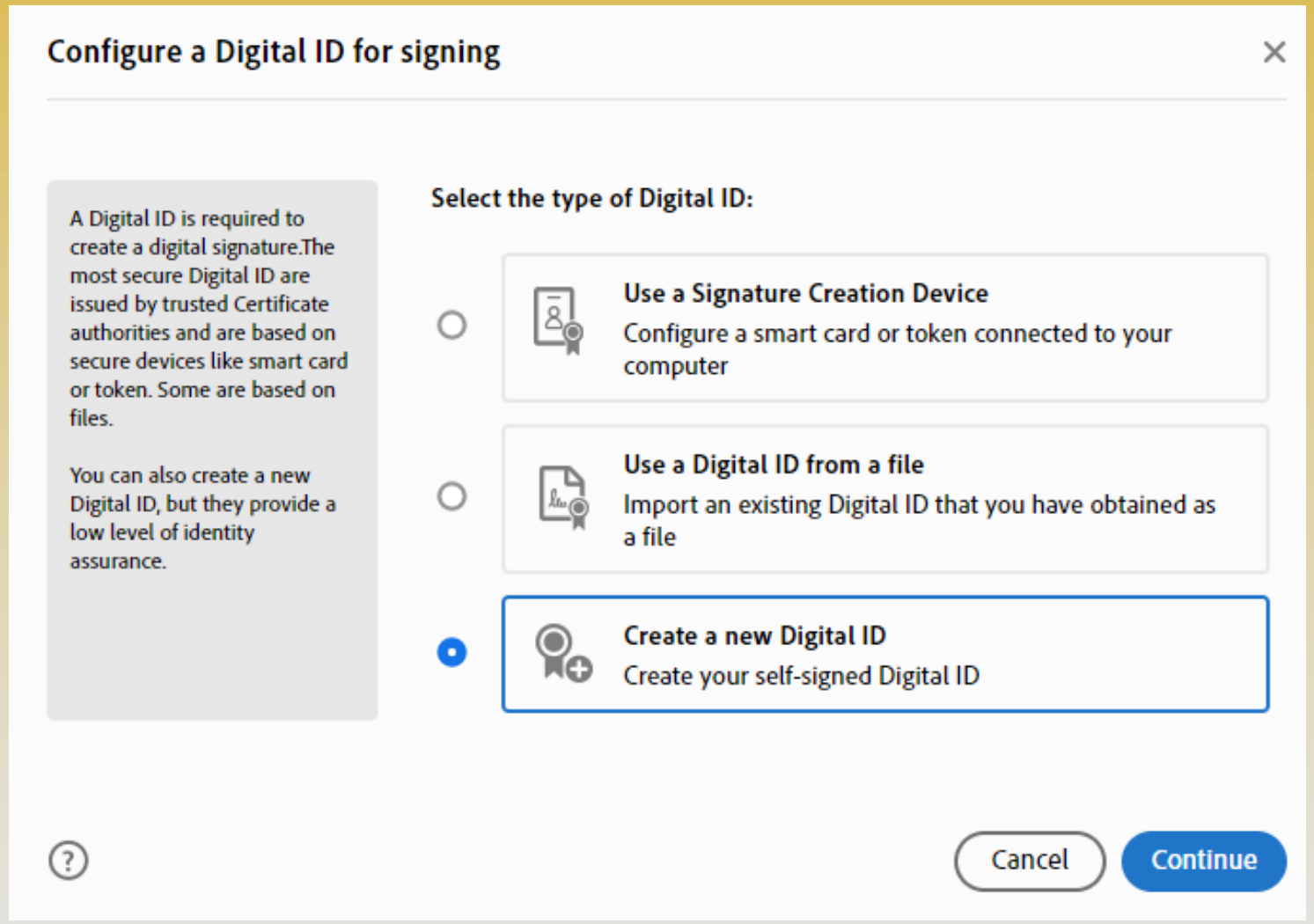
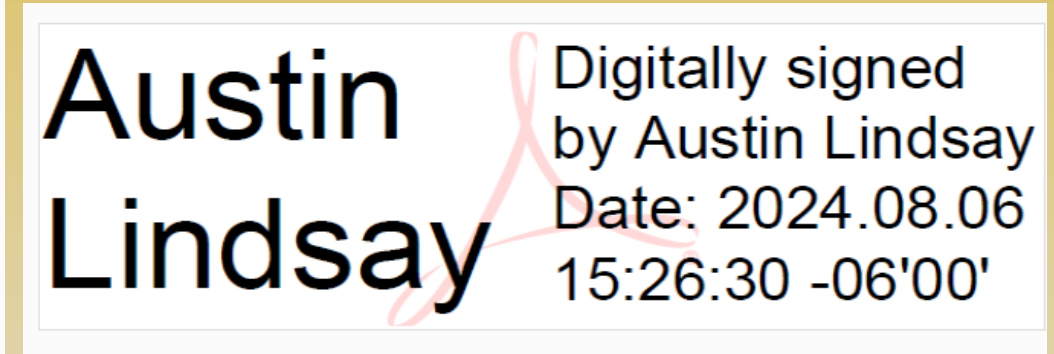
Demystifying Digital Signatures

Austin Lindsay
Information Security Officer
austin.lindsay@mt.gov
444-5476

CHRISTI JACOBSEN
MONTANA SECRETARY OF STATE

Digital Signature





CHRISTI JACOBSEN
MONTANA SECRETARY OF STATE

Digital Signatures for Remote Notarization

MCA 1-5-603 (12)(c)

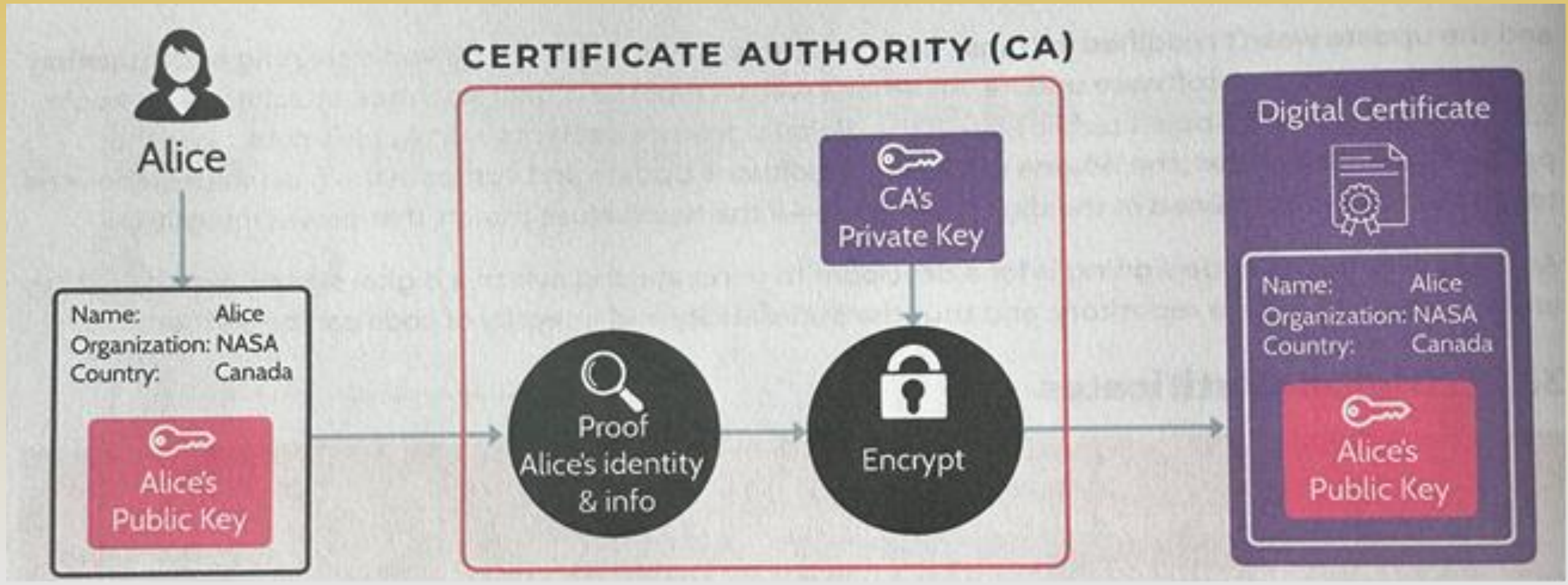
If a principal or witness is appearing by means of communication technology, a notarial officer has **satisfactory evidence** of the **identity** of the individual if the notarial officer can identify the individual by **two or more** different types of technologies, processes, or services approved by the secretary of state, such as:

- dynamic knowledge-based authentication assessment
- **valid public key certificate**
- identity proofing
- remote presentation
- credential analysis
- any other means prescribed in rule by the Secretary of State.

CHRISTI JACOBSEN
MONTANA SECRETARY OF STATE

Digital Certificate/Public Key Certificate

Digital Signatures tie identities to documents
Digital Certificates tie identities to digital signatures



3 Digital Signature Services

Integrity

- Verifies the document has not been altered after being digital signed and sent to the receiver.

Authenticity

- Verifies that the document was signed and sent by the claimed source.

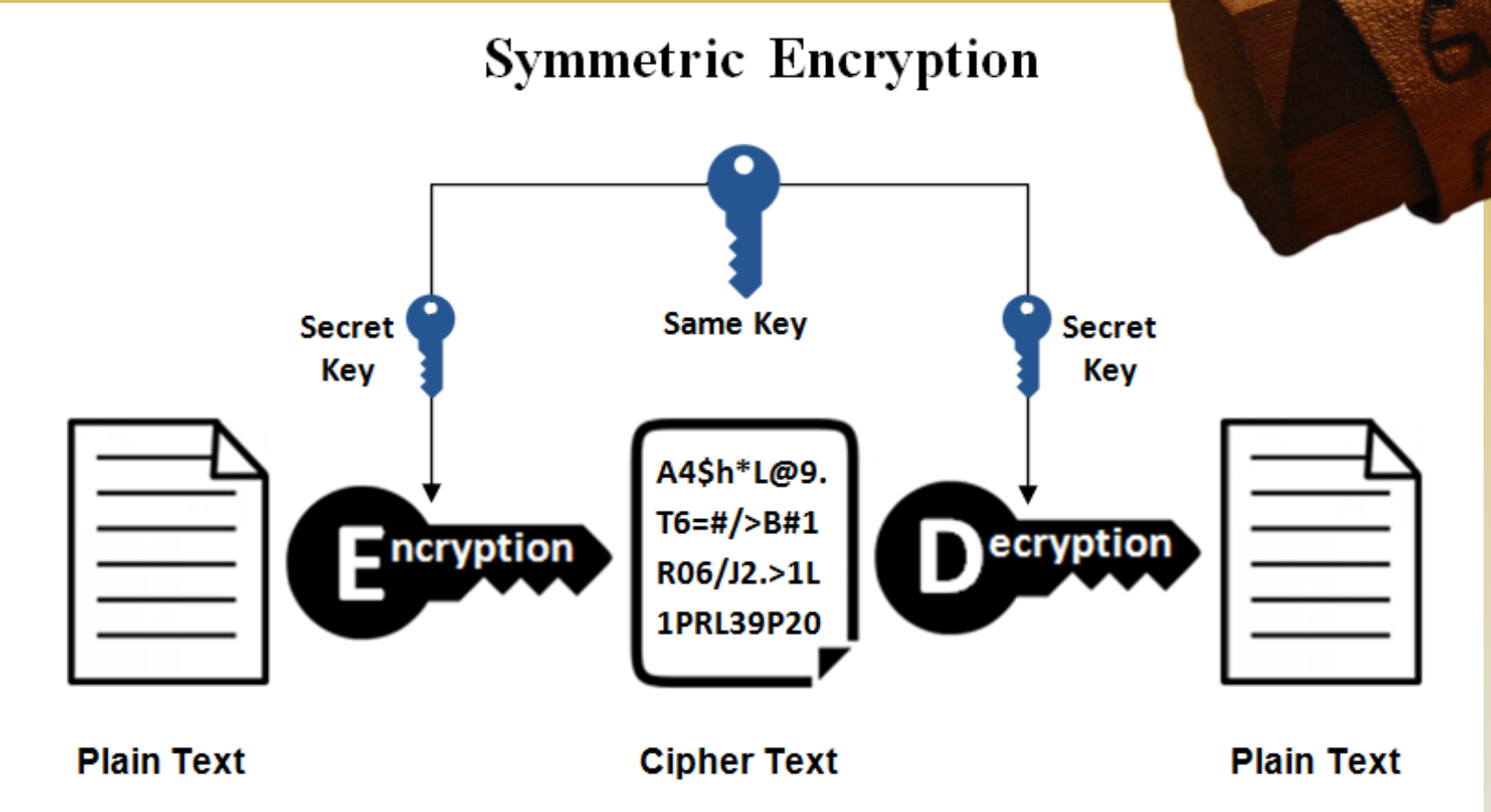
Non-repudiation

- The signer/sender can not deny sending/signing the unchanged document.
- Non-repudiation is achieved if integrity and authenticity are both achieved.

CHRISTI JACOBSEN
MONTANA SECRETARY OF STATE

Symmetric Cryptography

Ancient Greek Scytale

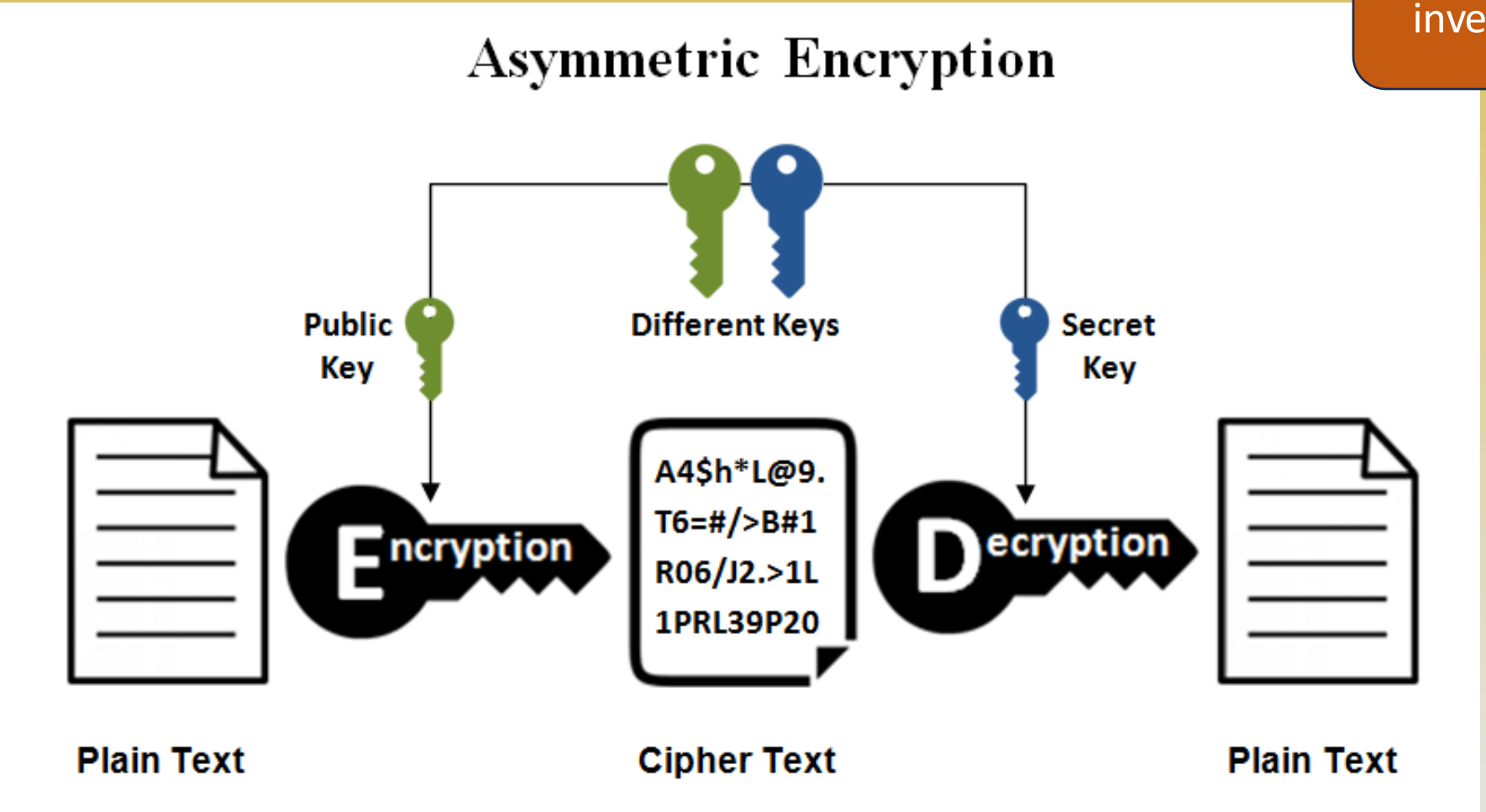


CHRISTI JACOBSEN
MONTANA SECRETARY OF STATE

Asymmetric Cryptography

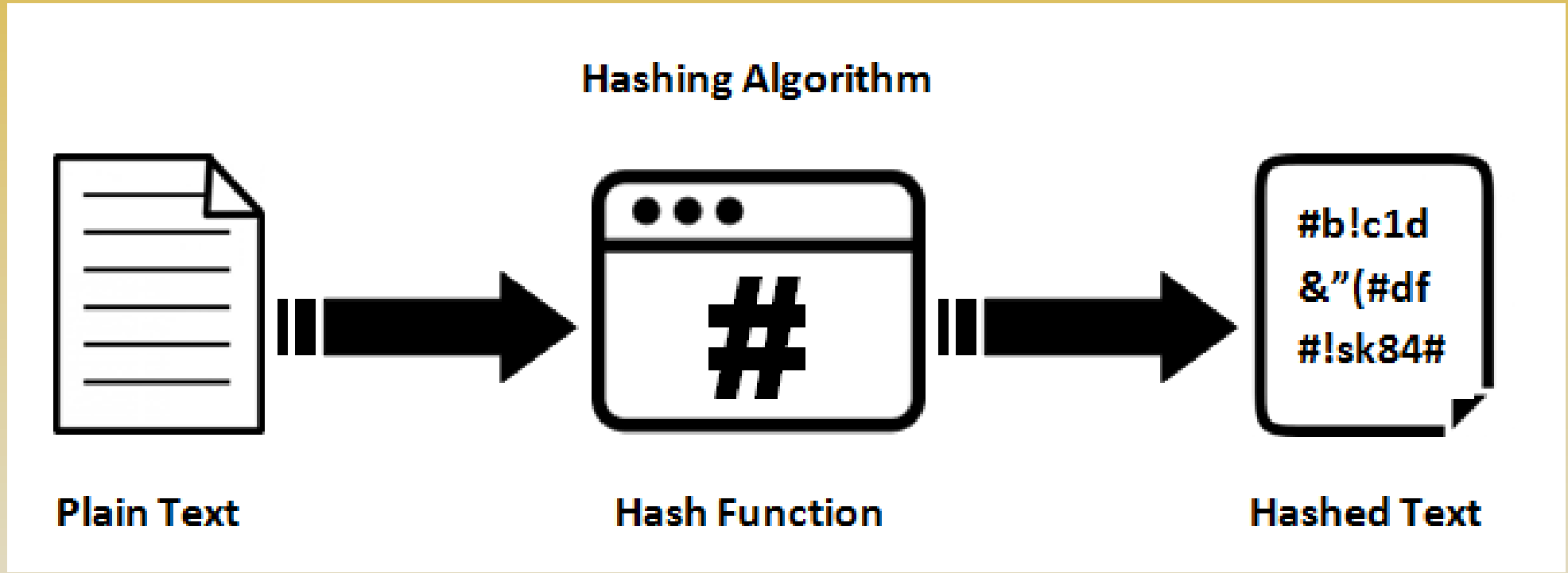
also known as public-key cryptography

RSA algorithm invented in 1976



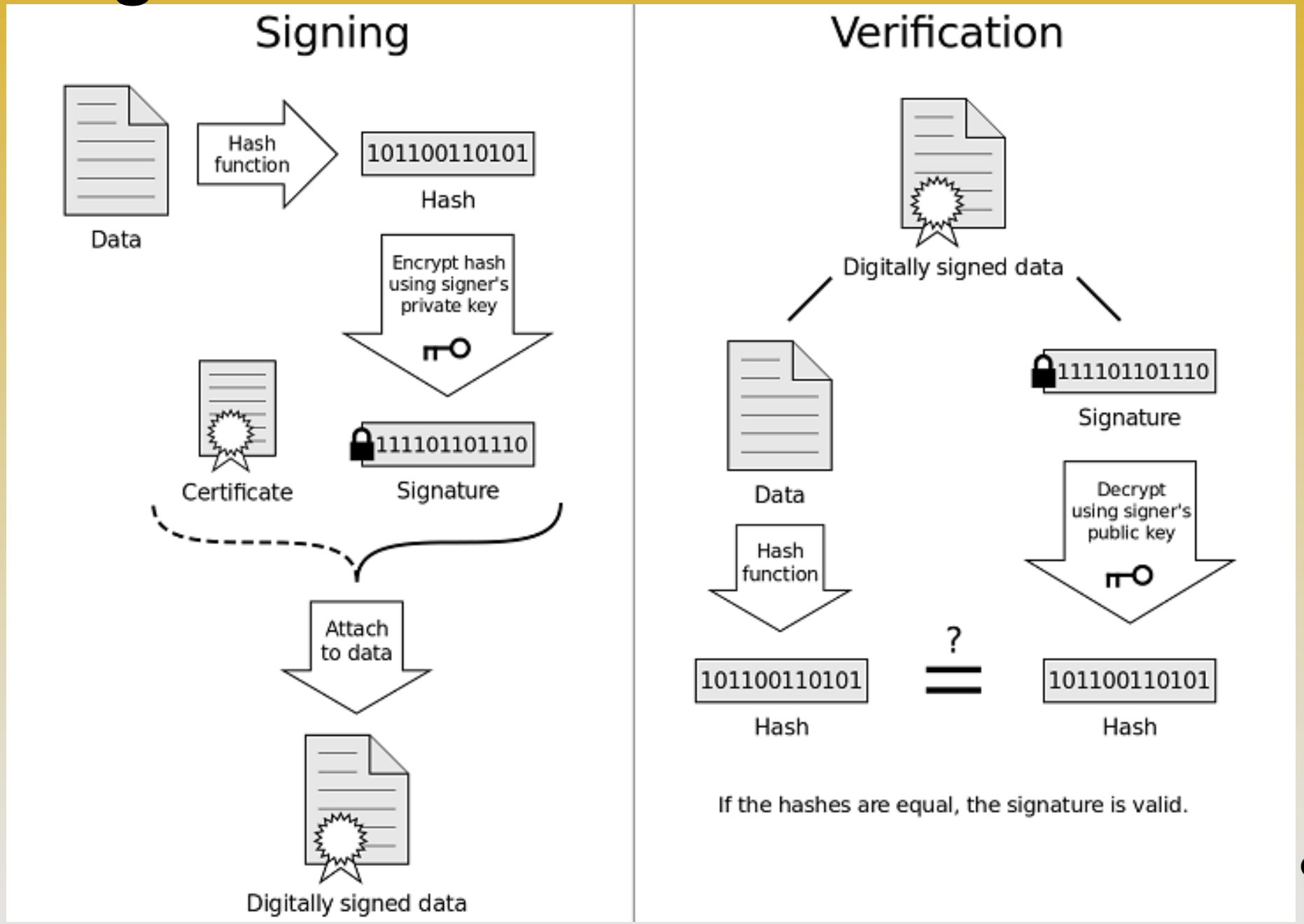
CHRISTI JACOBSEN
MONTANA SECRETARY OF STATE

Hashing



CHRISTI JACOBSEN
MONTANA SECRETARY OF STATE

Digital Signatures



CHRISTI JACOBSEN
MONTANA SECRETARY OF STATE

3 Digital Signature Services

Integrity

- Verifies the document has not been altered after being digital signed and sent to the receiver.

Authenticity

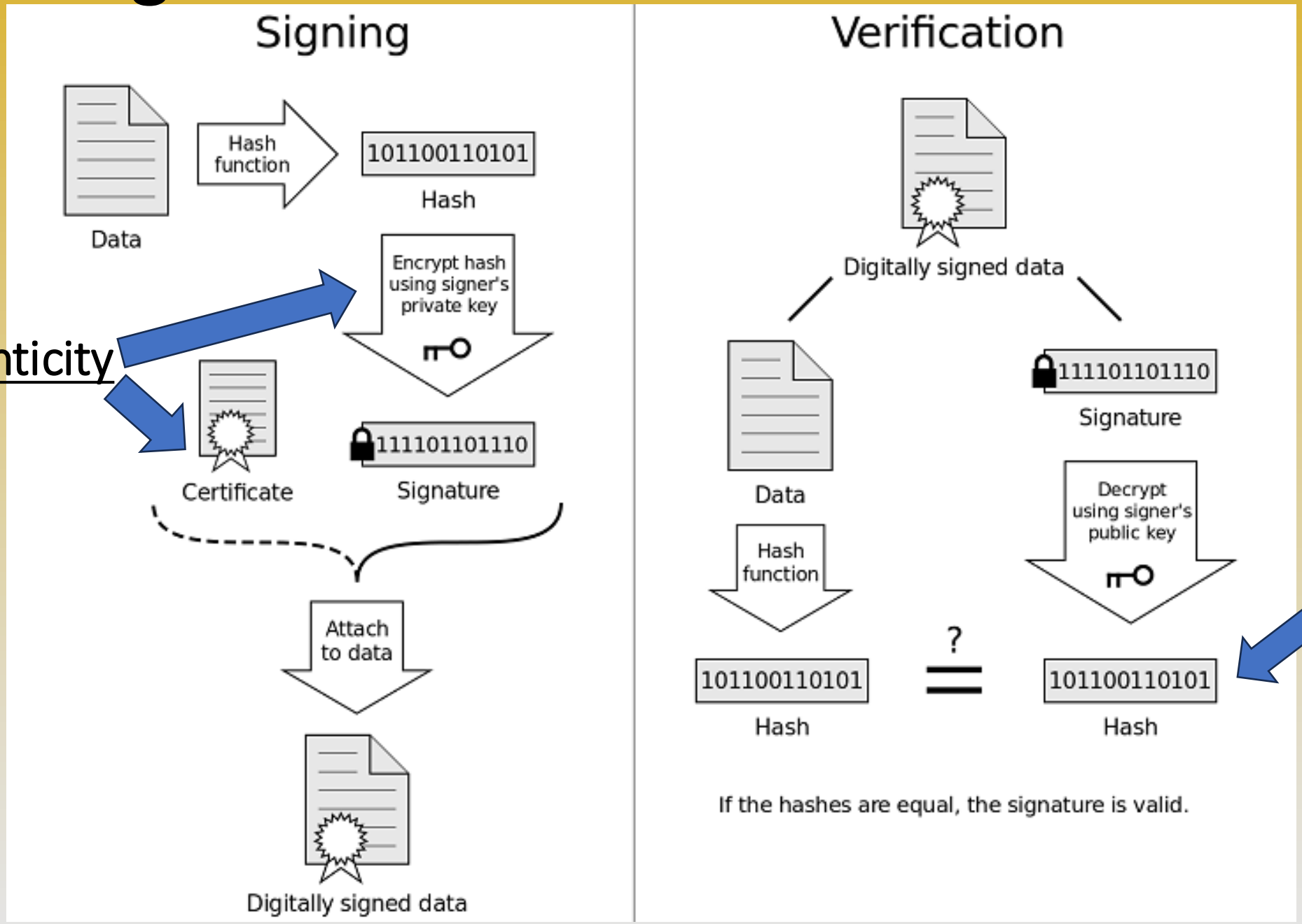
- Verifies that the document was signed and sent by the claimed source.

Non-repudiation

- The signer/sender can not deny sending/signing the unchanged document.
- Non-repudiation is achieved if integrity and authenticity are both achieved.

CHRISTI JACOBSEN
MONTANA SECRETARY OF STATE

Digital Signatures



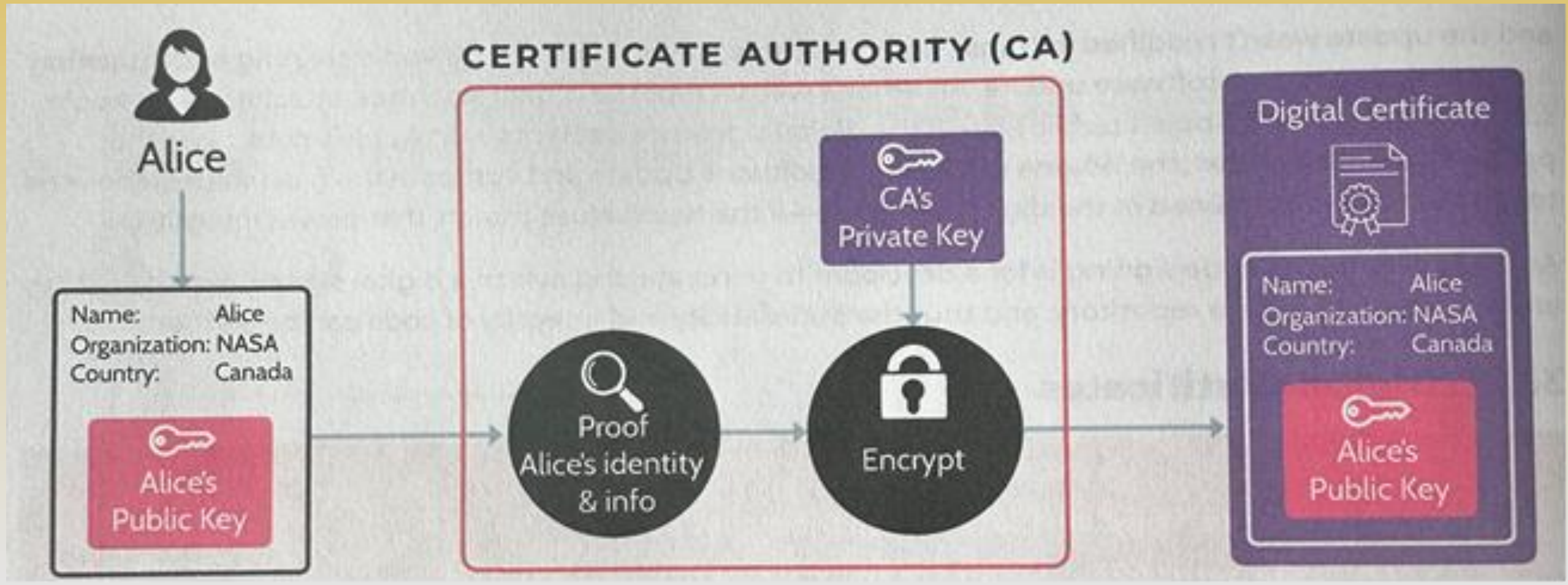
Authenticity

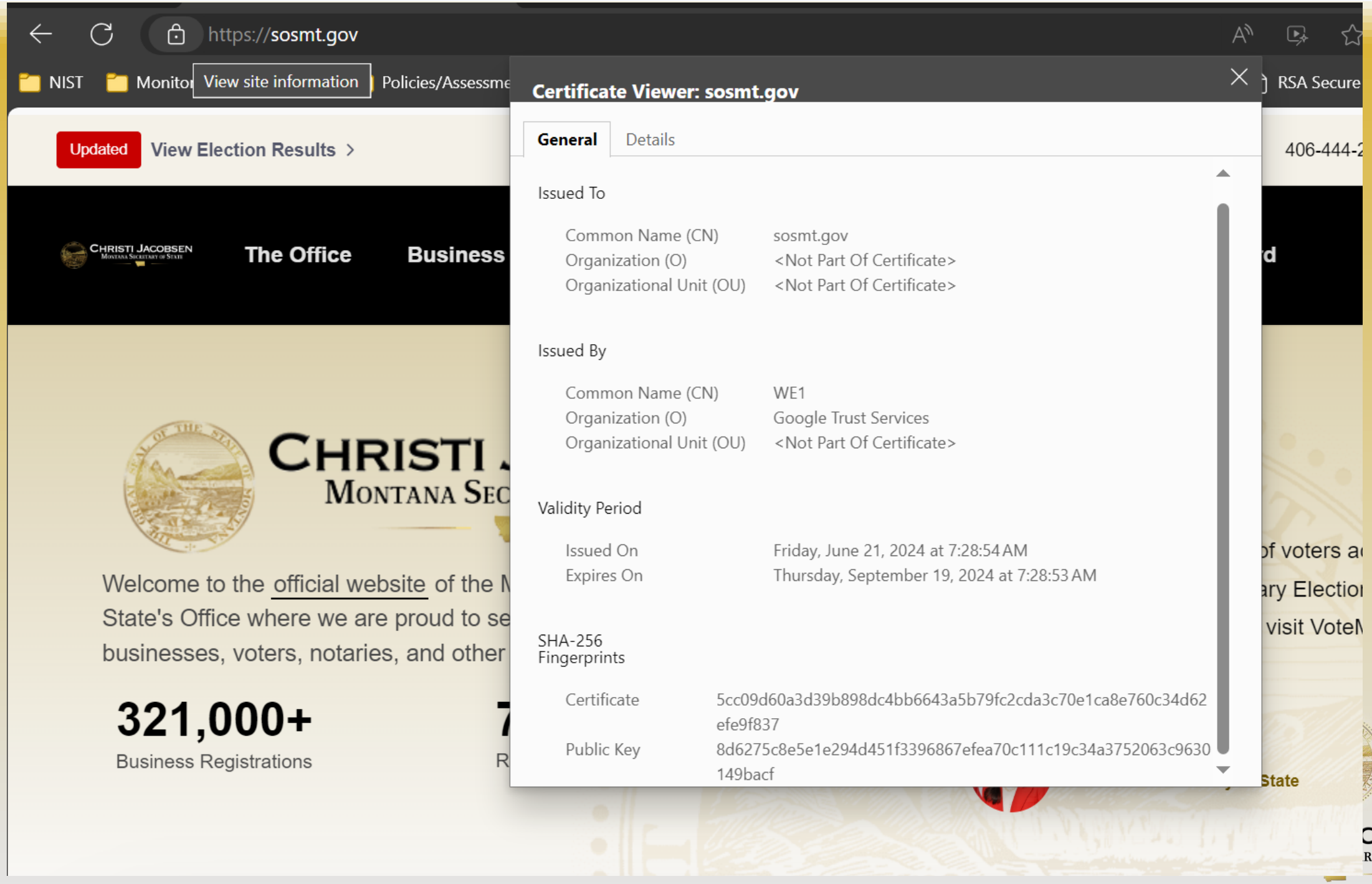
Integrity

CHRISTI JACOBSEN
MONTANA SECRETARY OF STATE

Digital Certificate/Public Key Certificate

Digital Signatures tie identities to documents
Digital Certificates tie identities to digital signatures




https://sosmt.gov
NIST
Monitor
View site information
Policies/Assessme
RSA Secure
Certificate Viewer: sosmt.gov
General
Details
Issued To
Common Name (CN) sosmt.gov
Organization (O) <Not Part Of Certificate>
Organizational Unit (OU) <Not Part Of Certificate>
Issued By
Common Name (CN) WE1
Organization (O) Google Trust Services
Organizational Unit (OU) <Not Part Of Certificate>
Validity Period
Issued On Friday, June 21, 2024 at 7:28:54 AM
Expires On Thursday, September 19, 2024 at 7:28:53 AM
SHA-256 Fingerprints
Certificate 5cc09d60a3d39b898dc4bb6643a5b79fc2cda3c70e1ca8e760c34d62efe9f837
Public Key 8d6275c8e5e1e294d451f3396867efea70c111c19c34a3752063c9630149bacf
Updated
View Election Results
406-444-2
CHRISTI JACOBSEN
MONTANA SECRETARY OF STATE
The Office
Business
Welcome to the official website of the M
State's Office where we are proud to se
businesses, voters, notaries, and other
321,000+
Business Registrations
CHRISTI J
MONTANA SEC
of voters a
ary Electio
visit VoteM
State
COBSEN
RY OF STATE

Quiz Question

Richard wants to digitally sign a message he's sending to Sue so that Sue can be sure the message came from him without modification while in transit. Which key should he use to encrypt the message digest?

A. Richard's public key
B. Richard's private key
C. Sue's public key
D. Sue's private key

Quiz Question

B. Richard's private key

Richard should encrypt the message digest with his own private key. When Sue receives the message, she will decrypt the digest with Richard's public key and then compute the digest herself. If the two digests match, she can be assured that the message truly originated from Richard.

CHRISTI JACOBSEN
MONTANA SECRETARY OF STATE

Austin Lindsay

Information Security Officer
austin.lindsay@mt.gov
444-5476