Figure 1: Digital Identity Authentication Mechanisms in Digital Financial Services

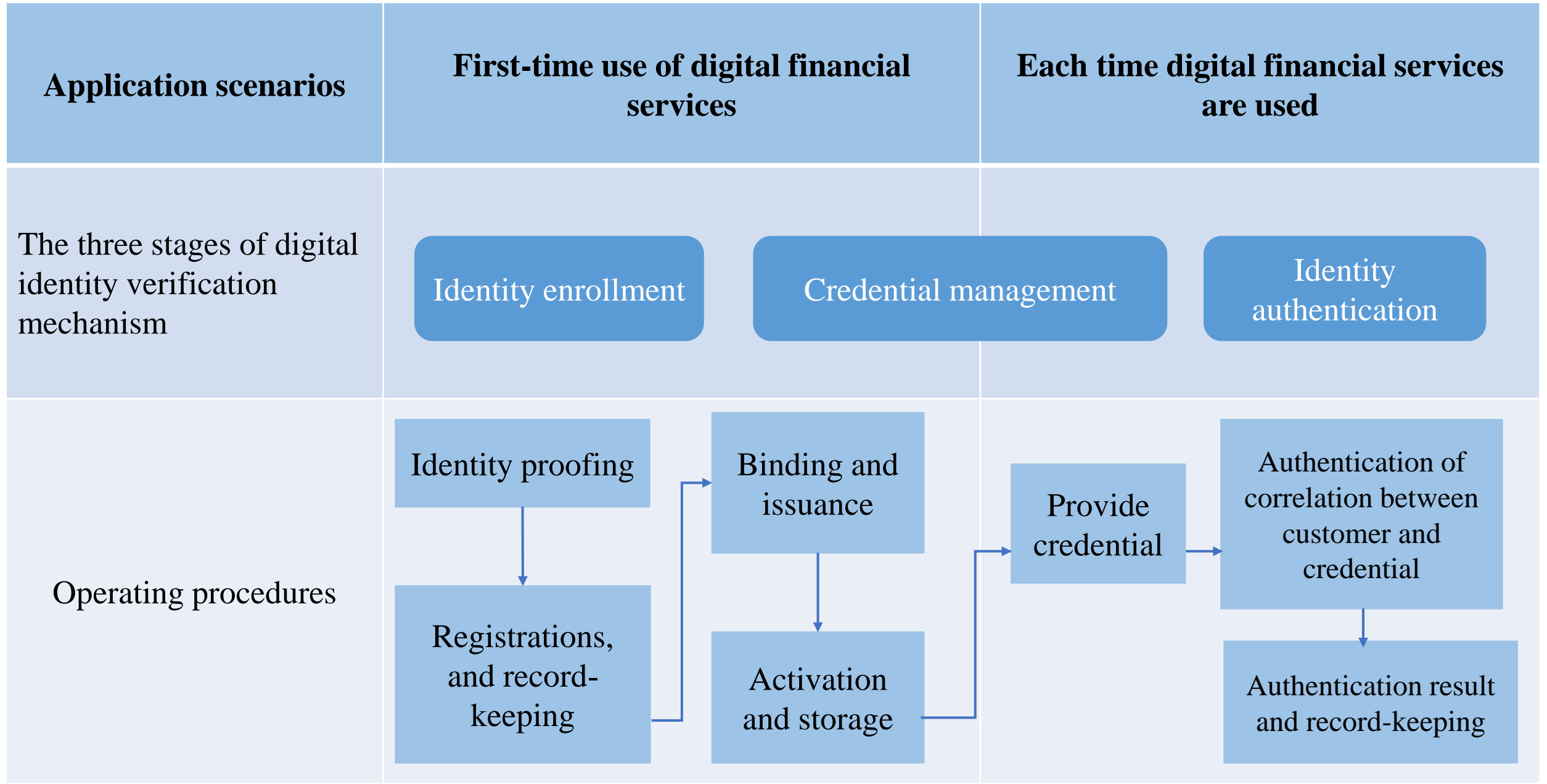| Application scenarios	First-time use of digital financial services	Each time digital financial services are used
The three stages of digital identity verification mechanism	Identity enrollment · Credential management	Identity authentication
Operating procedures	Identity proofing → Registrations, and record-keeping → Binding and issuance → Activation and storage → Provide credential	Authentication of correlation between customer and credential → Authentication result and record-keeping

Figure 2: Using an IC ATM card as a credential, and taking interbank withdrawals as an example, this figure illustrates the participants and operational procedures of digital identity authentication.

Trusted third party
Household registration authorities, Financial Information Service Co., Ltd. (FISC) and other credential authentication agencies

Identity enrollment operation 2
The issuing bank assists in verifying the customer's identity through a trusted third party.

Identity enrollment operation 1
① Customer applies for an IC ATM card through the issuing bank branch.

Credential
IC ATM Card

Customer

Issuing bank

Registration authority
Business unit

Credential management operation 1
④ The issuing bank produces, binds, and issues the IC ATM card.

Identity enrollment operation 3
③ Business unit completes registration and submits a request to the ATM card management unit for the customer to apply for an IC ATM card.

Credential management operation 2
⑤ Customer activates the IC ATM card according to the issuing bank's instructions.

Identity authentication operation 1
Customer makes a service request to another bank and uses the IC ATM card for identity verification.

Credential service provider
ATM card management entity

Credential management operation 3
⑥ The ATM card management unit transmits the customer's identity information and corresponding credential data to the verification services host server.

Identity authentication operation 2
Other banks submit a request to the issuing bank for identity verification of the customer.

Relying party
Other banks

ATM of other banks

FISC

Interbank service server

Verifier
Verification services host server

Identity authentication operation 3
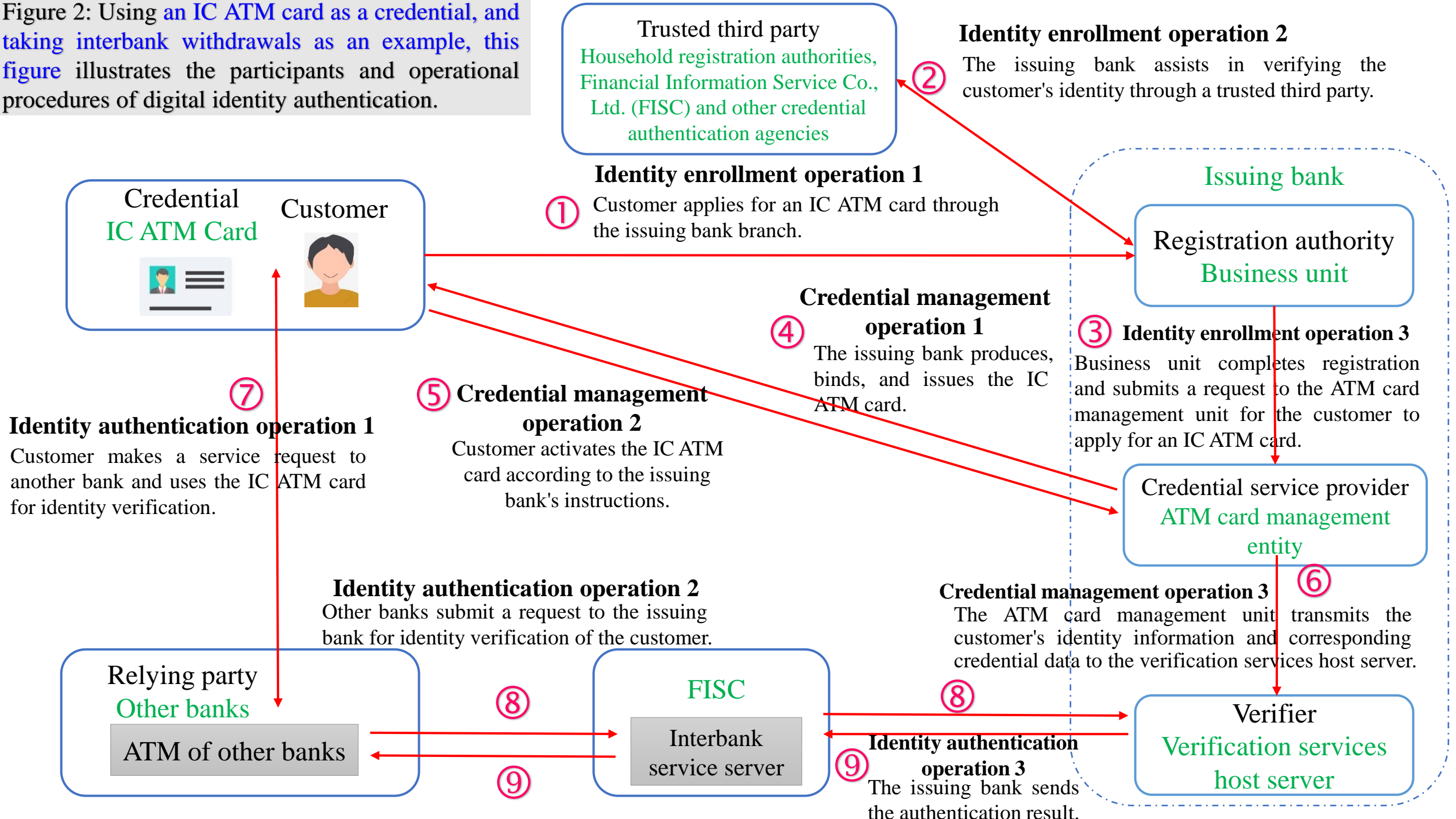⑨ The issuing bank sends the authentication result.

Figure 3: Using the order placement certificate of a securities (or futures) broker as a credential, and taking electronic trading as an example, this figures illustrates the participants and operating procedures of digital identity authentication.

Trusted third party
Household registration authorities, Financial Information Service Co., Ltd. (FISC) and other credential authentication agencies

Identity enrollment operation 2

The securities (or futures) firm assists in verifying the customer's identity through a trusted third party.

Credential management operation 1

The customer enters their member account and password, generates a key pair, and submits a certificate application to the registration authority.

① **Identity enrollment operation 1**

The customer applies to open an account at a securities (or futures) firm either in person or online.

Securities broker (or futures broker)

Credential
Order placement certificate of a securities (or futures) broker

④ Customer

③ **Identity enrollment operation 3**

The securities (or futures) firm completes the customer's identity verification and provides a member account and password.

Registration authority
Certificate Registration Authority

⑥ **Credential management operation 3**

The customer downloads the certificate from the certificate registration authority.

⑤ **Credential management operation 2**

The registration authority submits an application to the certificate authority and receives a response.

⑤

Certificate Authority

⑦ **Identity authentication operation 1**

The customer requests electronic trading services from the securities (or futures) firm and presents the trading certificate for transaction verification.

Credential service provider
The order placement certificate management entity of the securities (or futures) firm

⑨ **Identity authentication operation 3**

The securities (or futures) firm's internal security system requests the certificate revocation list (CRL) from the certificate authority.

Securities broker (or futures broker)

⑧ **Identity authentication operation 2**

The securities (or futures) firm's internal security system verifies the validity and accuracy of the certificate signature.

Securities broker (or futures broker)

Relying party
Business unit
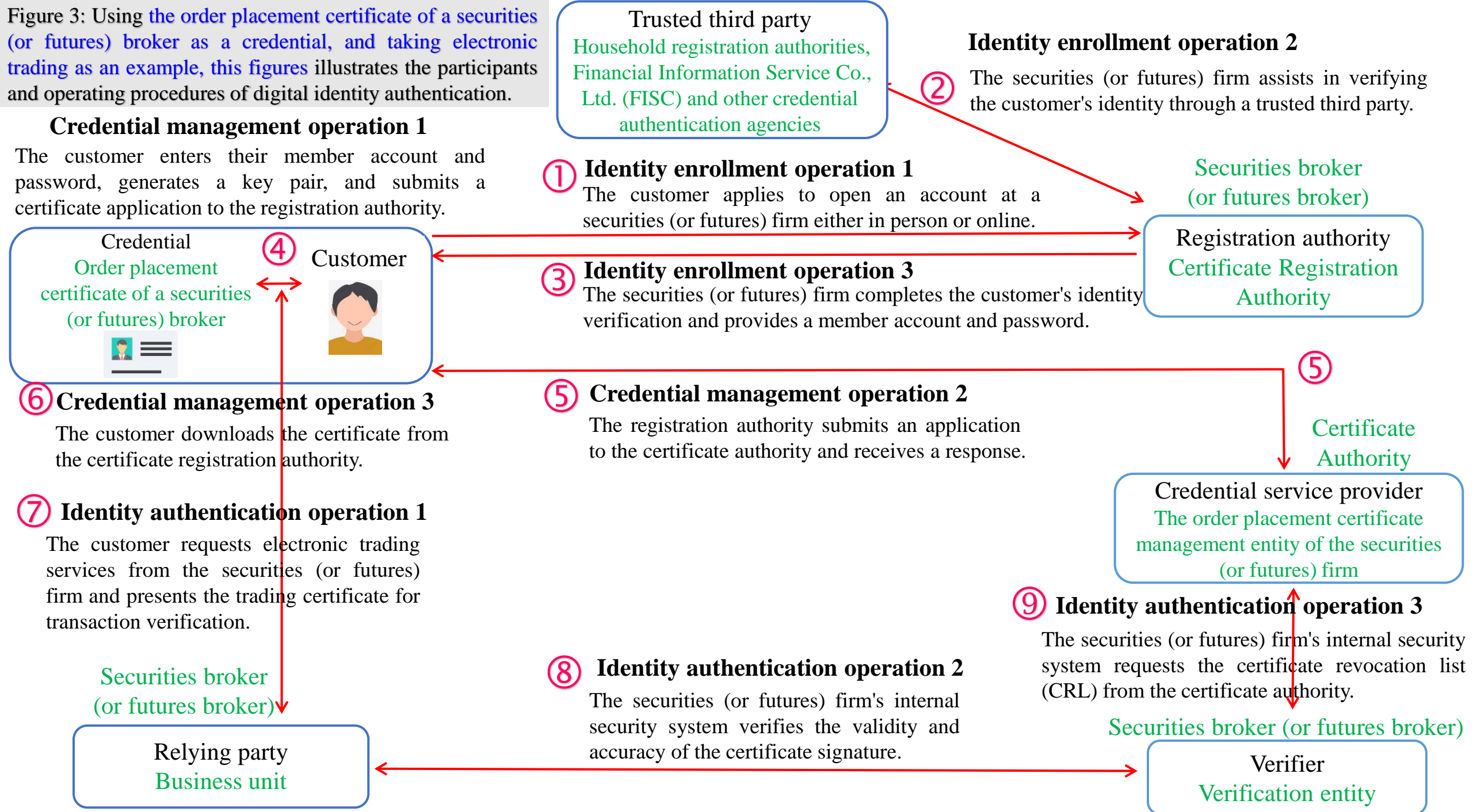
Verifier
Verification entity

Figure 4: Using Financial Fast-ID as a credential, and taking the provision of financial services as an example, this figure illustrates the participants and operational procedures of digital identity authentication.

Trusted third party
Household registration authorities, Taiwan Clearing House, Financial Information Service Co., Ltd. (FISC) and other credential authentication agencies

According to Section 2, Item 1, Subitem 3, and Section 3 of the "Guidelines for Security Control by Financial Institutions of Rapid Identity Verification Mechanisms": Identity verification should be conducted using in-person verification, IC Citizen Digital Certificates, or IC ATM cards.

② **Identity enrollment operation 2**
Financial institution A assists in verifying the customer's identity through a trusted third party.

Identity enrollment operation 1
① The customer applies for the Financial Fast-ID registration service through financial institution A.

Credential management operation 2
⑤ The customer's mobile device generates the Financial Fast-ID key pair, with the private key stored on the mobile device.

Credential
Financial Fast-ID

Customer

④ **Credential management operation 1**
Financial institution A requests the customer to generate the keys for the asymmetric encryption and decryption system.

Financial Institution A

Registration authority
Operation unit
③

Identity enrollment operation 3
The operations unit completes the registration and submits a request to the Financial Fast-ID service management unit for the customer's application for the Financial Fast-ID service.

⑥ **Credential management operation 3**
The customer sends the public key of the Financial Fast-ID key pair to financial institution A for safekeeping.

⑧ **Identity authentication operation 1**

The customer submits a service request to financial institution B and uses Financial Fast-ID for identity verification.

⑩ **Identity authentication operation 3**
Financial institution A performs identity verification for the customer using Financial Fast-ID.

Credential service provider
Financial Fast-ID management entity

Credential management operation 4
⑦ The Financial Fast-ID service management unit transmits the customer's identity information and corresponding credential details to the verification service of the Financial Fast-ID platform server.

Relying party
Financial Institution B

The online interface of financial institution B

⑨ **Identity authentication operation 2**
Financial institution B requests financial institution A to verify the customer's identity.

Verifier
Verification services
Financial Fast-ID server

⑪ **Identity authentication operation 4**
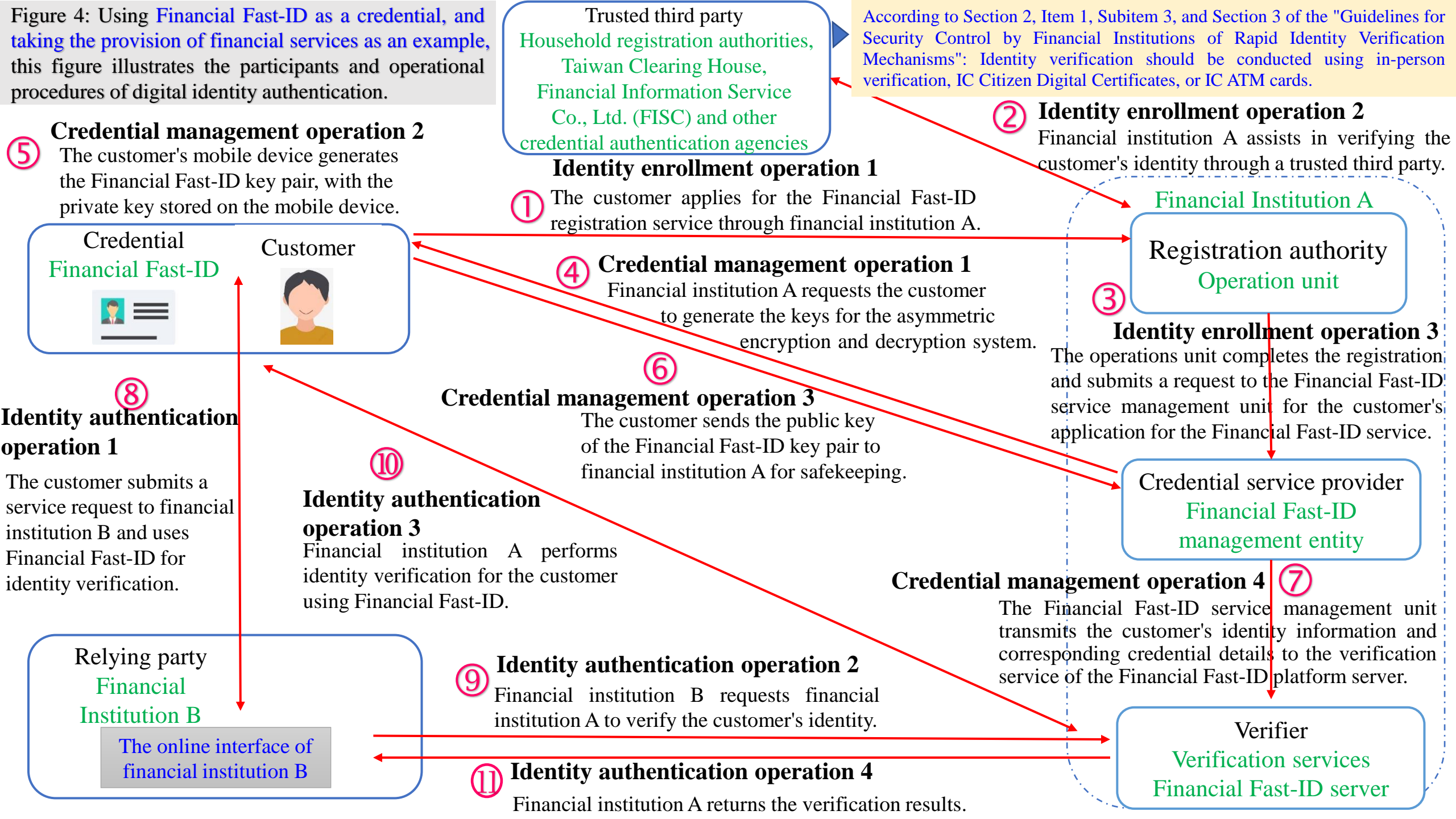Financial institution A returns the verification results.

Figure 5: uses a login to the insurance company's member area for digital identity verification to apply for claims and sign documents as an example, to illustrate the participants and operational procedures of digital identity authentication.

② Identity enrollment operation 2
The insurance passbook assists in verifying customers' identity through a trusted third party (e.g. personal identification certificates, IC ATM cards, enhanced MID, and mobile personal identification certificates).

Trusted third party
Household registration authorities, Taiwan Clearing House, Financial Information Service Co., Ltd. (FISC) and other credential authentication agencies

Credential
Account & password
Username
xxxxx
Customer

① Identity enrollment operation 1
1. The customer applies for an account online with an insurer.
2. The customer applies for an account online with an insurance passbook.

Registration authority
Insurers / Life Insurance Association
Insurance Passbook

③ Identity enrollment operation 3
1. The insurer completes the identity verification and provides the account and password.
2. The insurance passbook completes the identity verification and provides the account and password.

⑤ Credential management operation 1
After the customer completes the identity verification, they submit a certificate application to the registration authority.

Relying party
Business unit of the insurer

Sign the consent form

Credential service provider
Certificate authority
(certificate registration authority)

④ Identity authentication operation 1
The customer logs into the insurer's online portal, submits a claims application and chooses to verify their identity using either the enhanced MID or the insurance passbook account.

⑥ Credential management operation 2
The certificate authority returns the certificate for the customer to sign the documents.