ROK's legal aspects for digital authentication to support digital ICT services including Fintech services

25 April 2024

Heung Youl Youm, PhD/Professor
Soonchunhyang University, Korea (Republic of)
Chairman of ITU-T SG17 (Security)

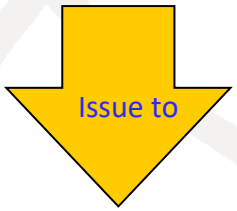
Digital identity

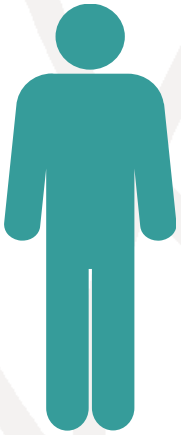
Identity verification

(Real world)

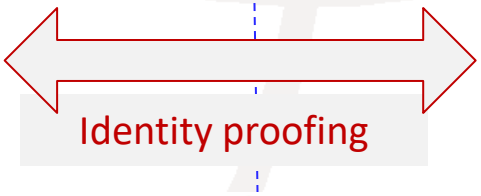
(Cyber space)

Government or authoritative authority





Physical identity card (document)



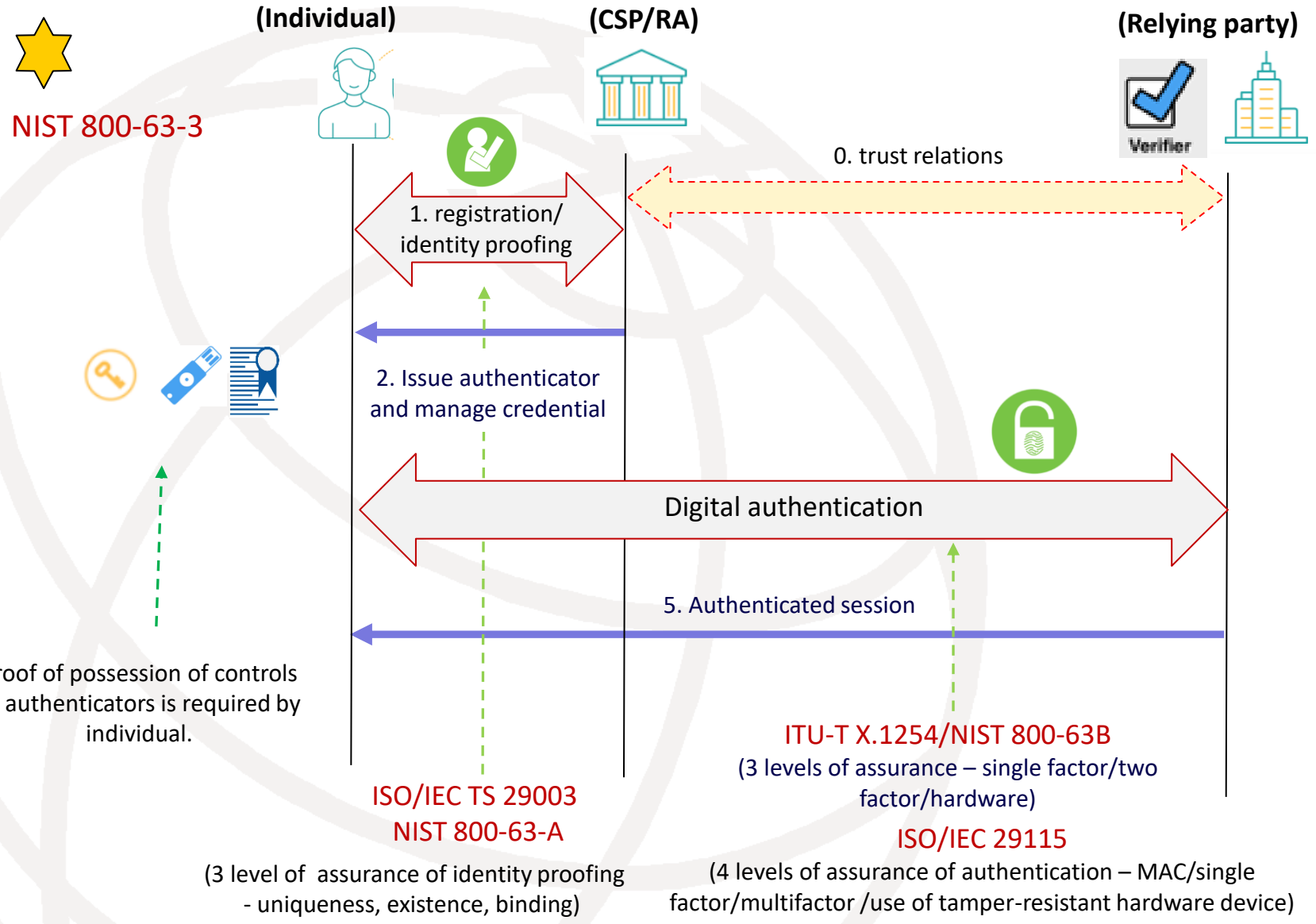
By registration authority

Relying party

Federation

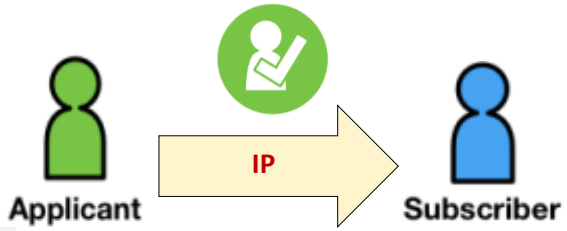
e-ID (such as Mobile driver's license)

Identity process and its assurance framework



Identity proofing - ISO/IEC 29003

- Specifies levels of identity proofing, and requirements to achieve these levels.
- Identity proofing refers to process by which the Registration Authority (RA) captures and verifies sufficient information to identify an entity to a specified or understood level of assurance
- Levels of identity proofing
  - Level 1
    - Identity is unique within the context
  - Level 2
    - Identity is unique within the context
    - some processes are undertaken to establish the identity exists
    - the subject has some binding to the identity. For example, using remote and PKI certificate.
  - Level 3
    - Identity is unique within the context
    - strong processes are undertaken to establish the identity exists
    - the subject has a strong binding to the identity. For example, using in-person and passport



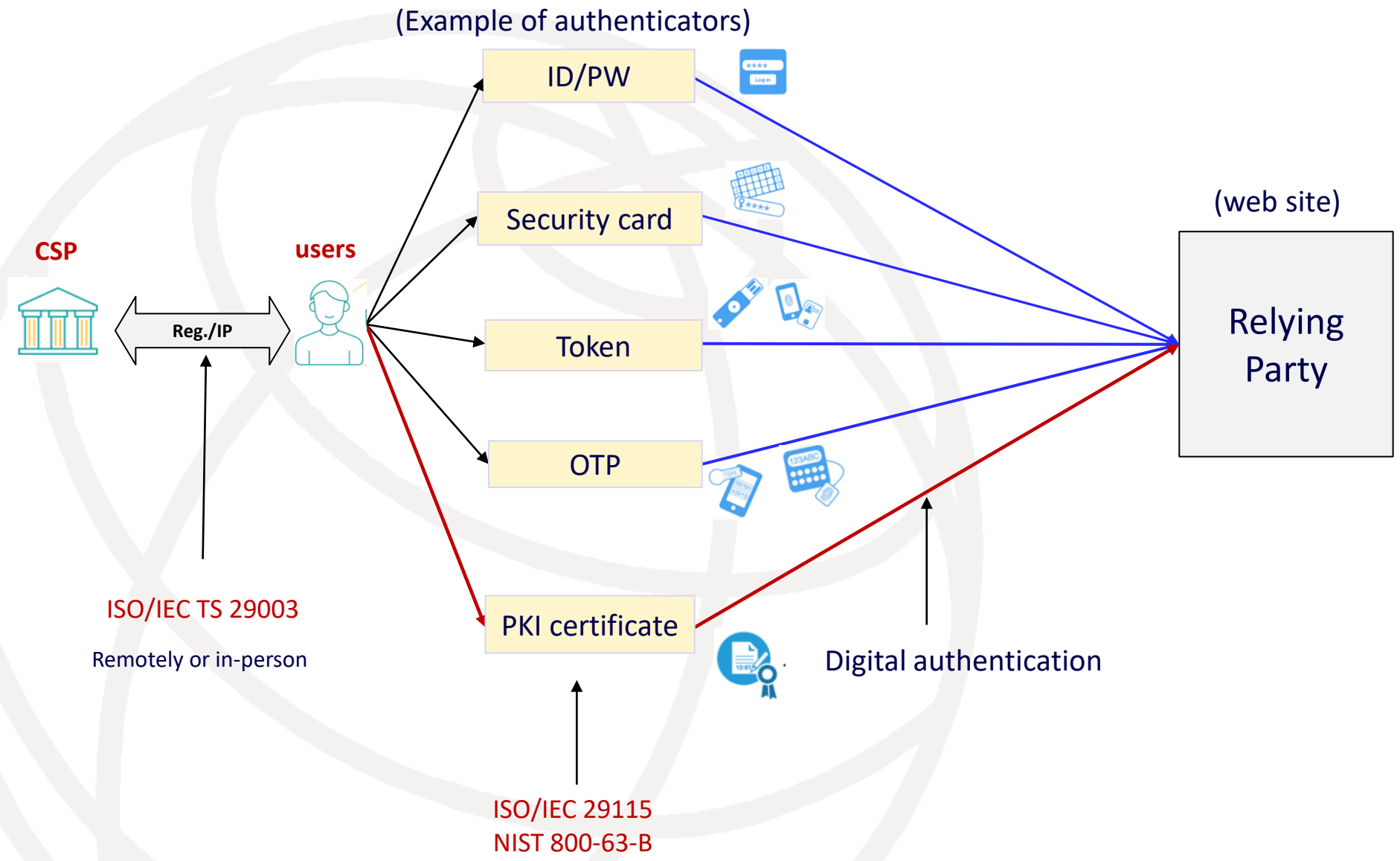
FIDO concepts for digital authentication

- Strong authentication =
  - Two factors

  - Public key cryptography such as digital signature algorithm

  - Providing usability and security for online authentication

PKI certificate as an authenticator



Terms and definitions related to identification and digital authentication

Terms relationships

Possession and control of private key should be proofed to relaying party

PKI services

Public key certificates issued by CA

Digital signature - data appended to a message, that allow the recipient of the message to verify the source of the message

- Message authentication
- Message integrity
- Non-repudiation

- Signature algorithms
- Hash algorithms
- Certificate profile in X.509

Electronic signature – data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign

(KR) Digital Signature act (DSA)

Electronic identification – the process of using person identification data in electronic form uniquely representing either a natural or legal person, or a natural person representing a legal person. (by e-IDAS)

Authentication - electronic process (1) that enables the electronic identification of a natural or legal person, or (2) to ensure the origin and integrity of data in electronic form to be confirmed.

(KR) Digital signature act, Act on information and communication network utilization and information protection etc. (ICT law)

Authentication - provision of assurance in the identity of an entity (ISO/IEC 29115)

Authentication factors

- something an entity knows
- something an entity has
- something an entity is

KR laws – digital authentication and electronic identification

Digital signature act (DSA)

Revised May 2020

- Purpose
  - to establish a basic framework for the system of digital signatures in order to ensure the safety and reliability of electronic messages and to promote their use, thereby accelerating informatization of the society and advancing public convenience
- Effectiveness of Digital Signature
- Establishment of policies for the development of electronic signatures
- Application for mediation of disputes related to electronic signatures
- Activation of the use of various electronic signature means
- Accreditation agency/assessment agency for digital signature service providers
- Identity verification, time stamping services of electronic document
- Protection of digital signature generated key

Electronic government act (EGA)

- Authentication of Administrative Digital Signatures(Article 29)
  - Any administrative agency may use an administrative digital signature.

Act on information and network utilization and information protection, etc. (ICT act)

- For electronic identification (so called IPIN)
- Designation of Identification Service Agencies (Article 23-3):
  - A plan for physical, technological, and administrative measures;
  - Technological and financial capability;
  - Appropriateness of the scale of facilities etc.
- Restrictions on Use of the Resident Registration Numbers (Article 23-2)
  - An identification service agency is allowed to collect or use users' resident registration numbers.
- Suspension of Identification Services and Revocation of Designation of Identification Service Agencies (Article 23-4)

Electronic financial transaction act (EFTA)

- Applicable to financial sectors
- Duty to Ensure Safety(Article 21)
  - Financial companies must comply with the standards set by the Financial Services Commission regarding authentication methods, such as the use of digital signature certificates issued under the Electronic Signature Act.

Components in KR laws

Completely revised on May 2020

Act on Information and network utilization and information security, etc.

- For electron identification service
- Identification service providers such as IPIN
- Various identity proofing methods
- Providing identification service to web sites

Digital signature act

- For digital signature service
- Designating digital signature service providers issuing certificates, known as CA
- Accreditation agency for assigning assessment organizations
- Assessment organizations for assigning accredited digital signature service providers
- Time stamping services of electronic documents

Electronic identification and digital signature procedure

Certificate issuing procedures according to “Digital signature act”

Registration/identity proofing by RA

(in person or remotely)

Issuing digital signature certificate by CA

For digital authentication

For generating digital signature of electronic document

IPIN (Internet Personal Identification Number)

Electronic identification procedures according to “Act on information and network utilization and information protection etc”

Electronic identification is conducted, when a user wants to register to web site.

The CI (connection information) + DI (domain information) are provided to local web sites.

(using certificate, SMS message, credit card number/PW for credit card, or account of identification service provider f user)

Identity proofing in advance through mobile phone/credit card/certificate registration in person

Key standards - digital signature and identity verification

Global laws and regulation

- (KR) Digital signature act (totally revised on May 2020 and put in force on December 2020)
- (EU) e-IDAS (electronic identification and trusted service) Regulation (July 2014)
- (USA) NIST, "Digital Identity Guidelines"

Major issues

Identity proofing

- (KR) digital signature act, Act on information and communication network utilization and information protection etc.
- (EU) e-identification part in eIDAS (2014.07.23)

Digital signature

- (KR) digital signature act
- (EU) Qualified trust service provider in e-IDAS (2014.07.23)

Authentication

- (KR) Act on information and communication network utilization and information protection etc
- (EU) e-identification part in eIDAS (2014.07.23)

Public key certificate

- (KR) digital signature act
- (EU) Qualified trust service provider in e-IDAS (2014.07.23)

International standard related to digital signature and authentication

- ISO/IEC TS 29003:2018
- ISO/IEC 29115:2013
- ITU-T X.1254(2013)
- NIST 800-63A (2017)
- ISO/IEC 24760-1/2/3

- ITU-T X.509 (2019)
- IETF RFC 3161(time stamping)

- ITU-T X.1254:2013
- ISO/IEC 29115: 2013
- ITU-T X.1403: 2020
- NIST 800-63-3 (2017)
- FIDO UAF/CTAP(U2F)
- ITU-T X.1277 / X.1278
- W3C Web Authentication

- ITU-T X.509 (2019)
- IETF RFC 5280 (PKI cert. and CRL)
- RFC 3161, Time Stamping Service

Concluding remark

- Legal measures are critical to address the risks in Fintech services, together with four countermeasures:
  - Technical measures, physical measures, organizational measures and people measures in ISO/IEC 27002
- Digital authentication and identity verification are key enablers for providing confidence and trust in the use of ICTs, especially for fintech services.
- Digital authentication and identity verification should be based on international standards:
  - Use of hardware-based module and secure zone in the mobile devices is preferred.
- FIDO specifications could meet enough security and usability of the digital authentication.

Thank you for your attention.