Keynote - Fintech security and decentralized identity

April 24, 2024

Heung Youl Youm, PhD.

Chairman, ITU-T SG17 (Security)

Director, SCH Cybersecurity research center

SOON CHUN HYANG UNIVERSITY

Fintech security

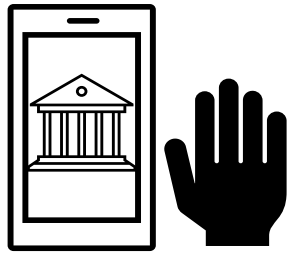
What is fintech services and are examples of service?

Definition by ITU-T X.1149

- Fintech refers to ICT technologies used by a financial industry to improve financial services. FinTech includes the applications, processes, products, or technology models in the financial services industry, composed of one or more financial technologies that are provided as an end-to-end process via the Internet.

Example of fintech services

- Mobile banks
- Mobile payments
- Cryptocurrency exchanges
- Insurtech (insurance + technology)
- Crowdfunding
- …

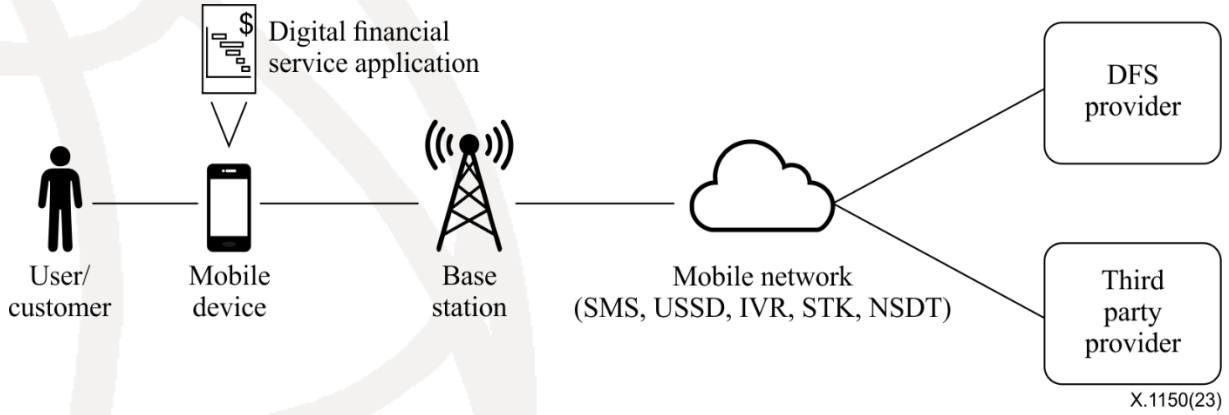


Security assurance framework for digital financial services in X.1150

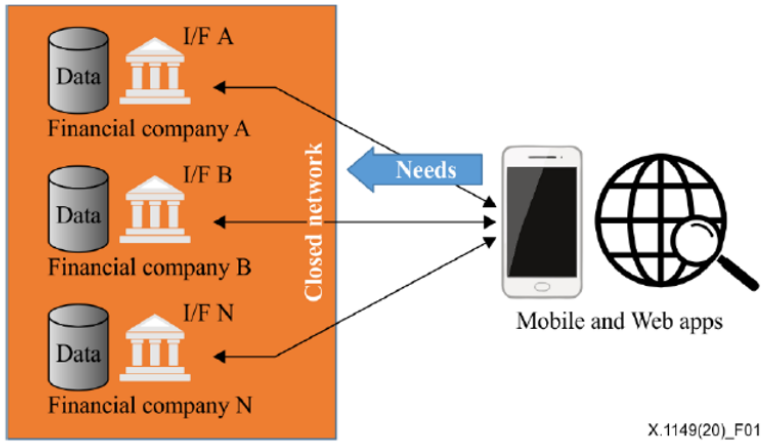
ITU-T X.1150

- Digital financial services (DFS) refers to the broad range of financial services accessed and delivered through digital channels, including payments, credit, savings, remittances, investing and insurance.

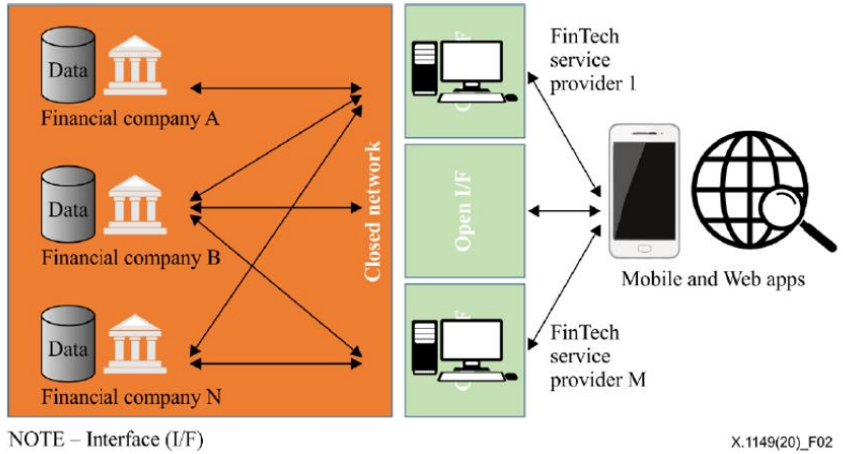
- It specifies a systematic security risk management process for identifying and assessing threats and vulnerabilities and identifies appropriate security controls to address vulnerabilities and mitigate risks.



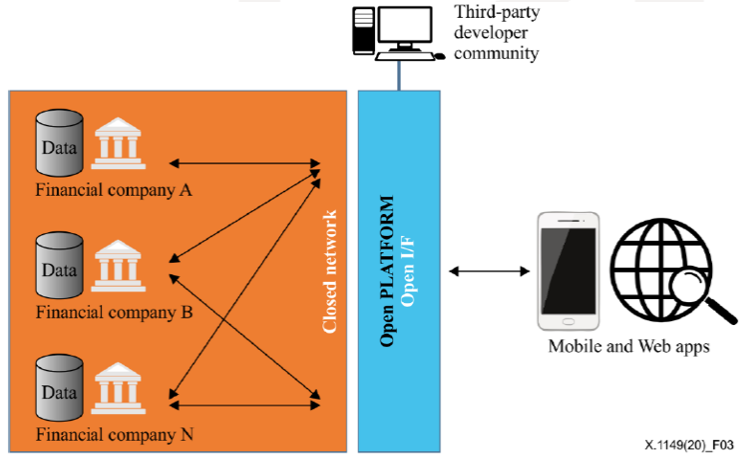
Reference architectures for Fintech services in X.1149



Architecture of digital financial services provided by traditional financial companies



Architecture with FinTech service providers



Open platform architecture for Fintech services

Cybersecurity challenges in Fintech services

Sophisticated cyber attacks from i.e. malware attacks including supply chain attacks

Third-party security risks from entities such as vendors, suppliers, partners, contractors.

Privacy breaches

Digital identity risks

Cloud-based security risks

Equifax Data breach in 2017

Who : Consumer credit reporting agency

Cause : failure to install the security updates of open-source software provided in a timely manner

Affected individual: Equifax announced a data breach that exposed the personal information of 147 million people

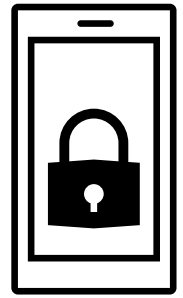
Date: September of 2017

Cybersecurity attacks trends

Targets are evolving, covering from critical infrastructure to fintech infrastructure, supply chain, sensitive data to classified data.

Attack techniques are evolving, i.e. use of generative AI

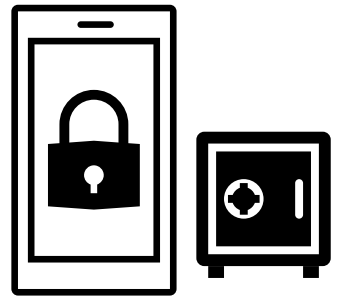
Purpose are diversified, for money, political reason, or social system destruction, etc.



Impacts (financial loss, reputational loss, compliance) are increasing and expanding.

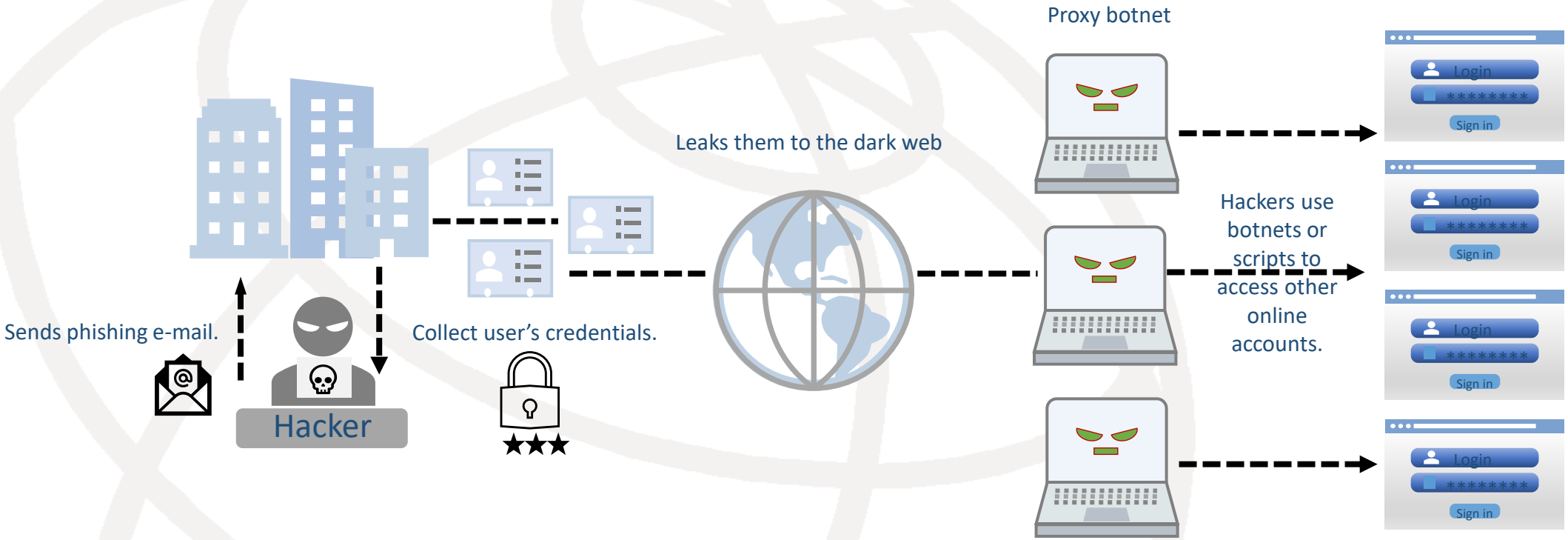
Four key security countermeasures for fintech service

- Use of a strong identity and authentication, i.e., multi-factor authentication.
- Use of zero-trust security architecture
- Use of software bill of material to address supply chain attacks
- Use of AI to improve the cybersecurity defense capabilities



Strengthen cybersecurity (in ISO/IEC 27001) and privacy protection capabilities (in ISO/IEC 27562) for all stakeholders providing fintech services.

Phishing and credential stuffing attacks

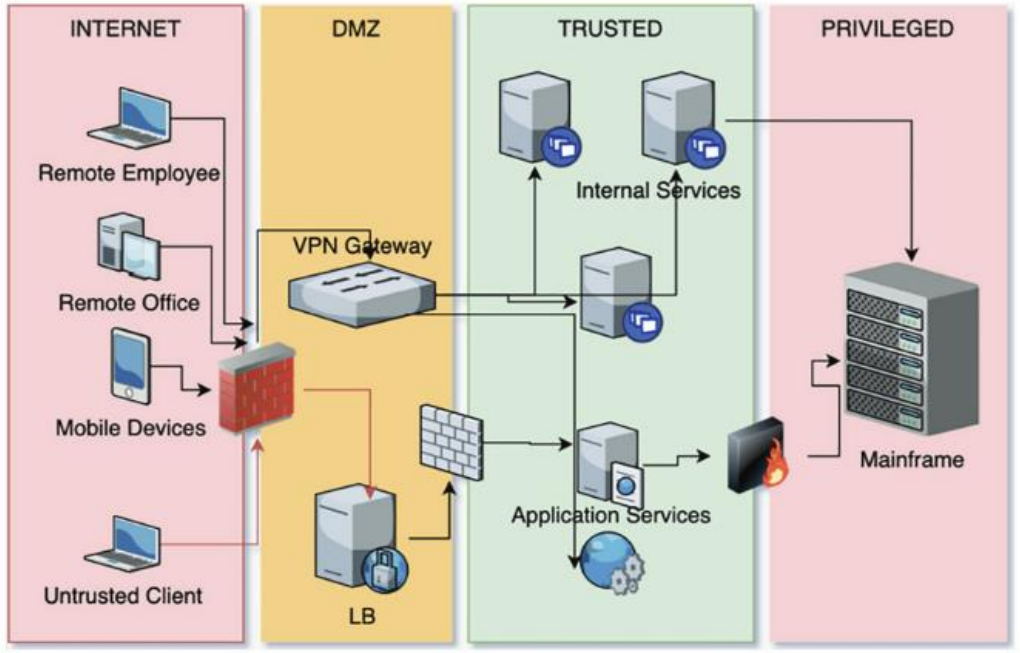


- How to do
  - Using compromised credentials
  - Accessing online accounts
  - using to proxy bots
- Measures by users
  - Use different passwords for different accounts
  - Quickly change your data breach account password
  - Usage of strong authentication based on multi-factor authentication.
- Measures by organizer
  - Training
  - Least Privilege Access Control
  - Multi-factor authentication- Monitoring and emergency response

Use of a strong authentication (FIDO passkey)

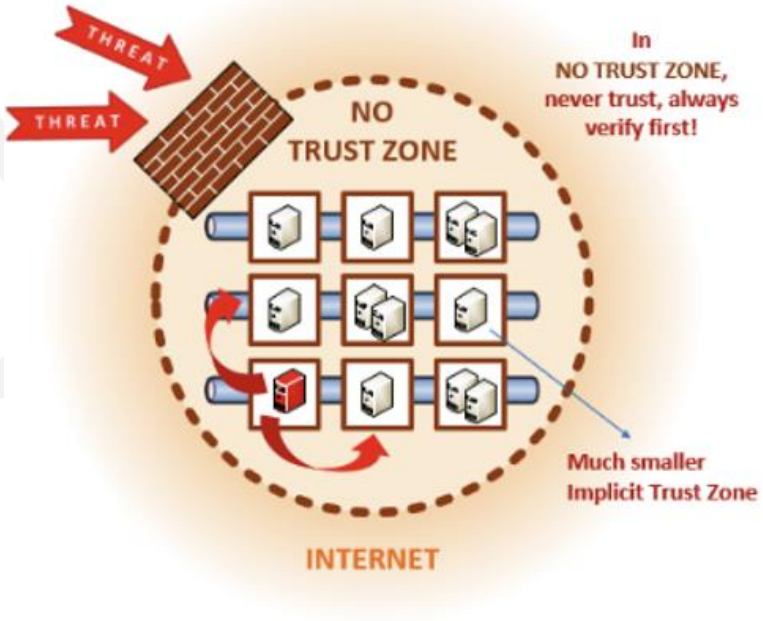
- Strong authentication =
  - Use of two factors 
  - At least one public-keys 
  - Resistant to phishing and man-in-the middle attacks

Use of zero-trust security architecture



* LB: Local Broker

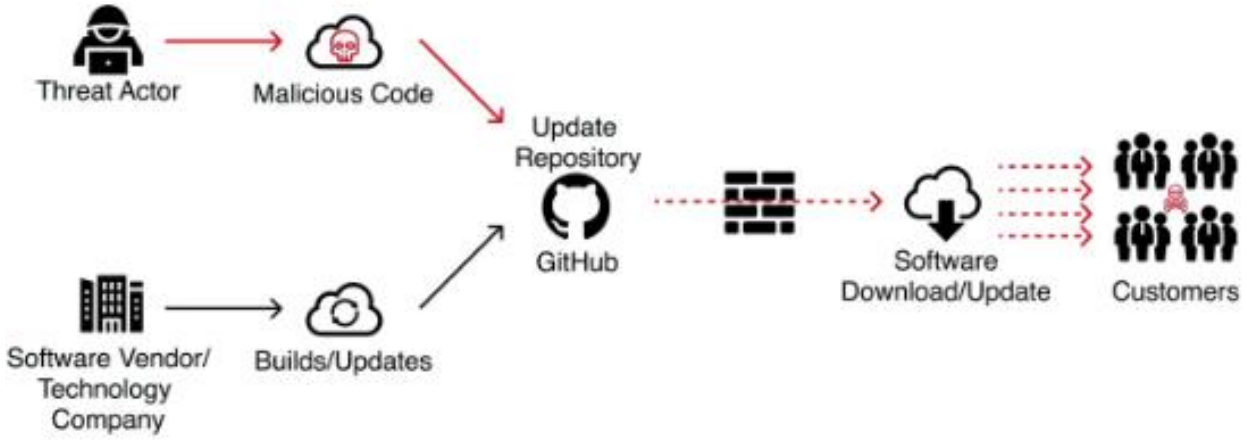
(Source: https://onlinelibrary.wiley.com/doi/epdf/10.1002/spy2.191)



(Source: NIST 800-63)

Use of software bill of material to address supply chain attacks

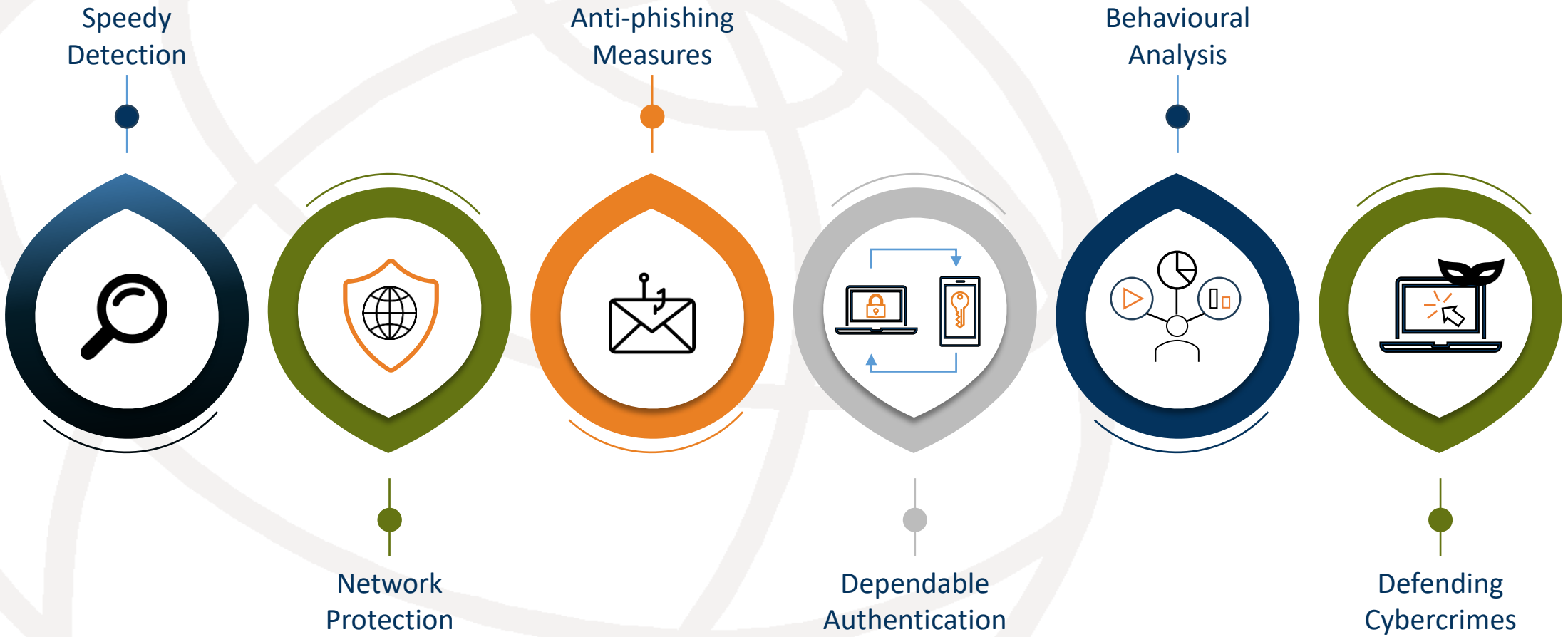
Software supply chain attacks



(Source: https://www.youtube.com/watch?v=KpvHL4cwFTI)

- A Software Bill of Materials (SBOM)
  - a comprehensive inventory that documents all the software components, libraries, frameworks, modules, and dependencies used in a particular software application or system
- Benefits of software bill of material
  - Enhanced security to detect and address security vulnerabilities
  - Risk managements to assess potential risks associated with third-party components.
  - Compliance and Licensing to facilitate compliance with software licenses and open-source licensing requirements.
  - Transparency and Accountability

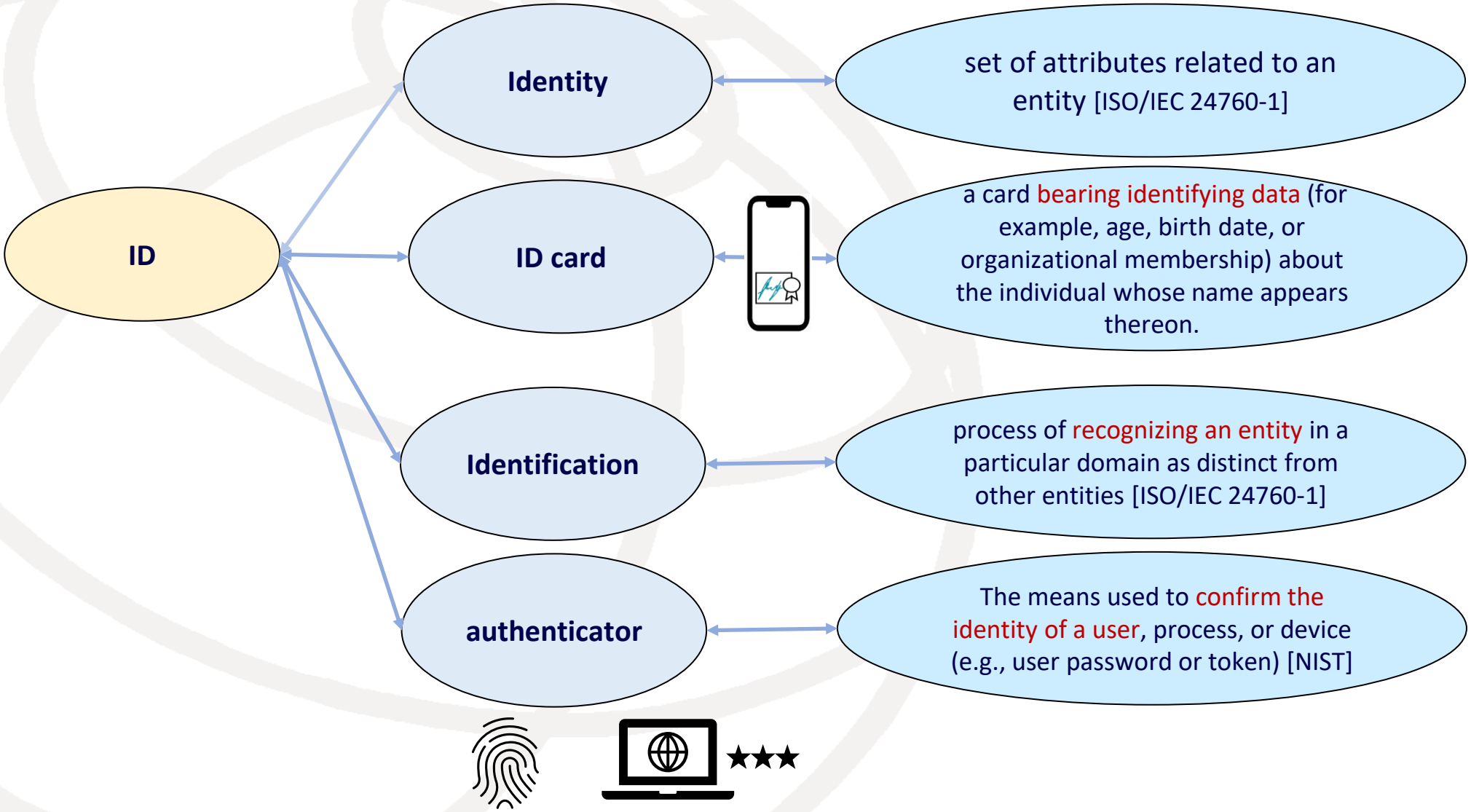
Use of AI/ML to improve the cybersecurity defense capabilities



(Source: Timothy Joseph, The Future of AI in Cyber Security Testing: Unlock the Potential)

Decentralized identity

What is identity?



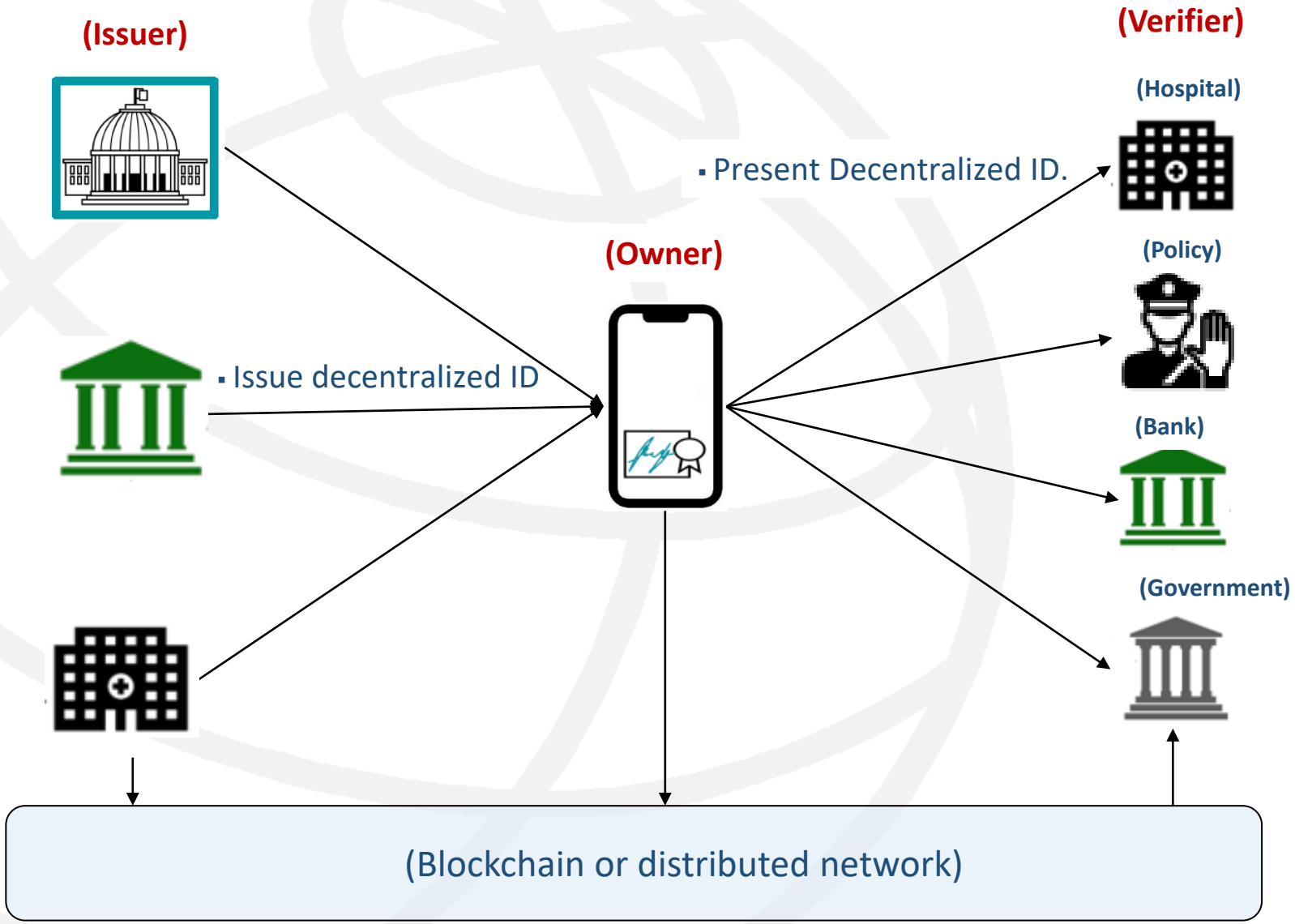
Physical ID

Physical ID attributes

- identifying subject (for example, photo, name, unique identifier)
- Issuing organization (for example, Ministry of internal affair, ministry of transportation)
- Type of credential (example, passport, driver's license)
- Credential attribute (for example, nationality, birth of date)
- Other attribute (for example, validity period)

(Source: https://www.w3.org/TR/vc-data-model/)

Self-sovereign user-centric decentralized Identity



Underlying key technologies behind the Blockchain

1

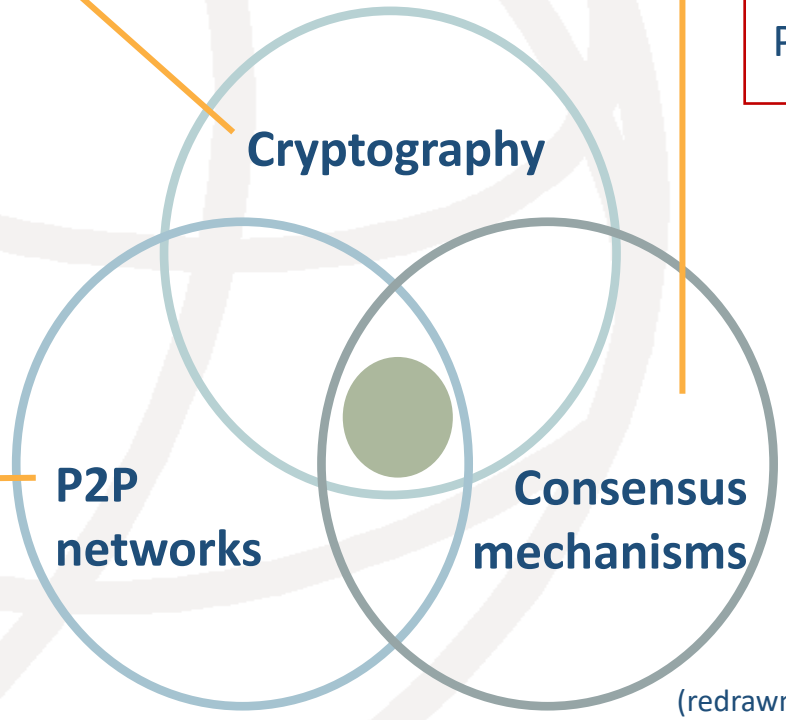
Use of public key cryptography and cryptographic hash functions: essential for transparency & privacy.

2

Nodes of P2P Network validate transactions by consensus, following economic incentive mechanisms (Proof of Work, Proof of Stake, etc.).

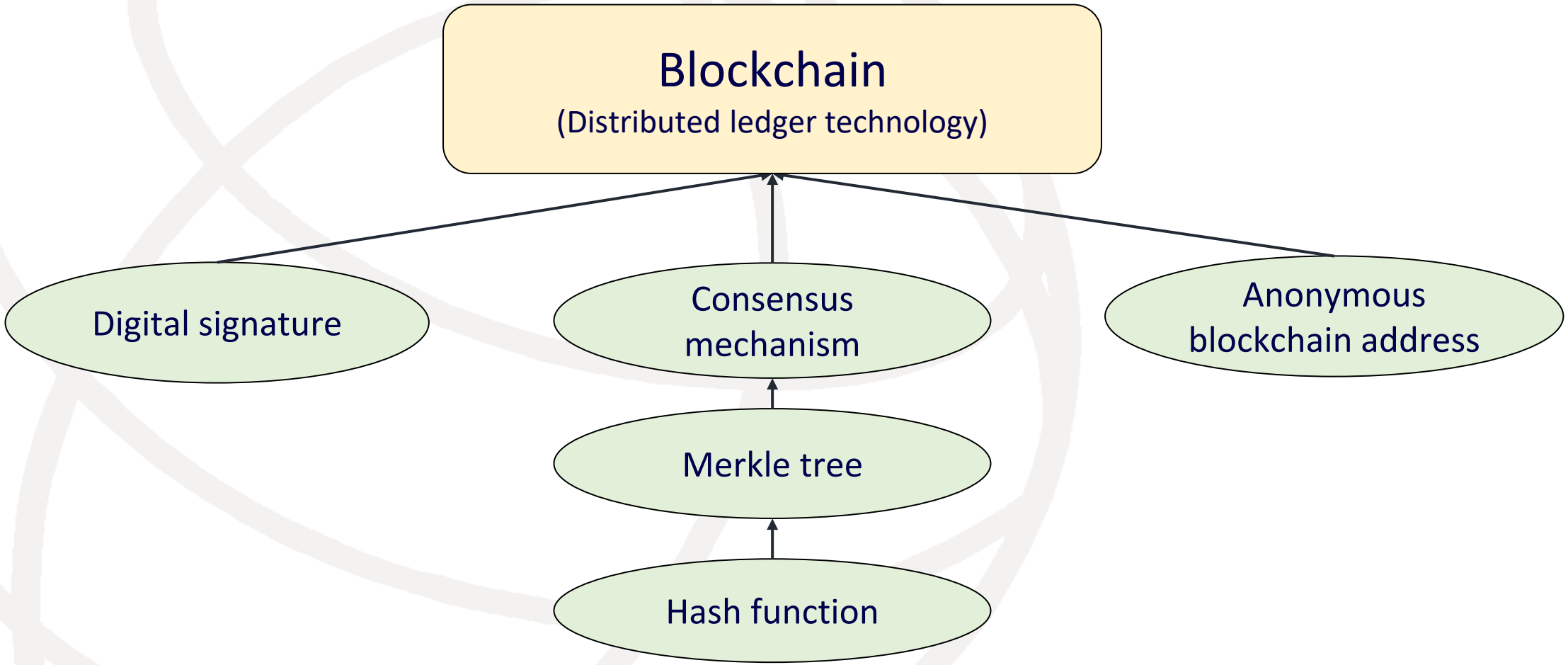
3

Every node of network acts as a client as well as server, holding identical copies of the application state.

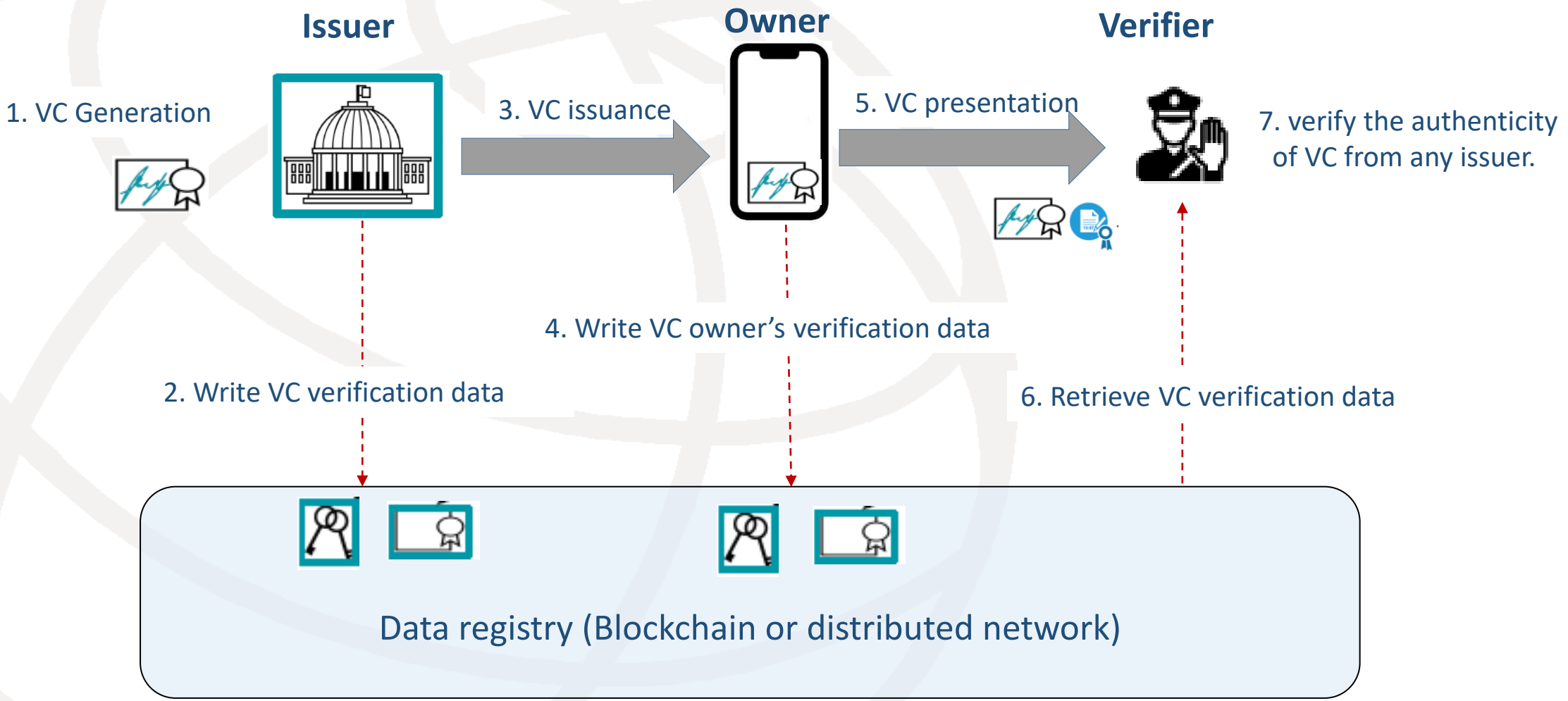


(redrawn and adapted from https://blockchainhub.net/blockchain-intro/)

Hierarchy of cryptographic primitives for Blockchain

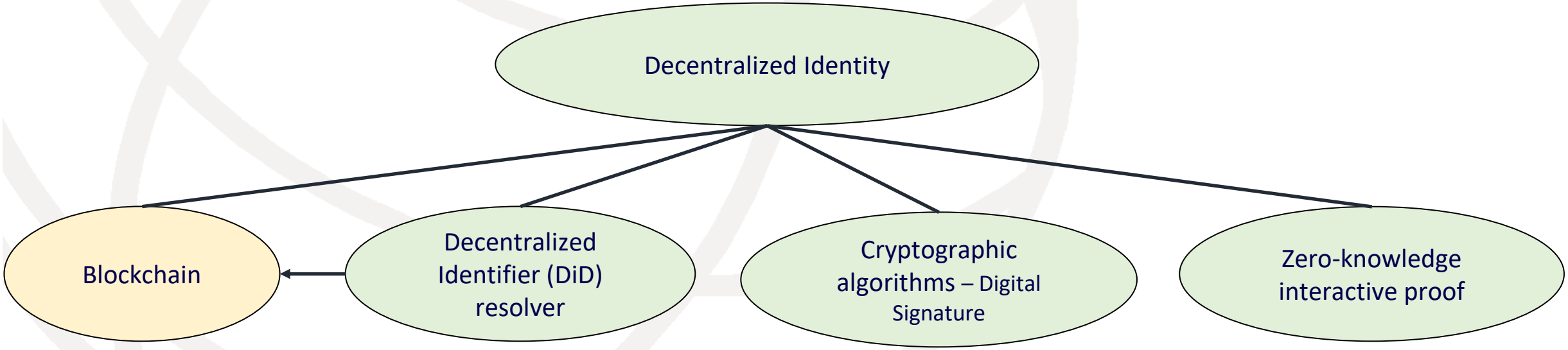


Ecosystem for decentralized identity



Key primitives for Decentralized Identity

- Decentralized ID
  - Decentralized identifier
    - A new type of identifier that is globally unique, resolvable with high availability, and cryptographically verifiable
  - Verifiable credential
    - A tamper-evident credential that has authorship that can be cryptographically verified.



A use case - Korea COVID-19 certificate service

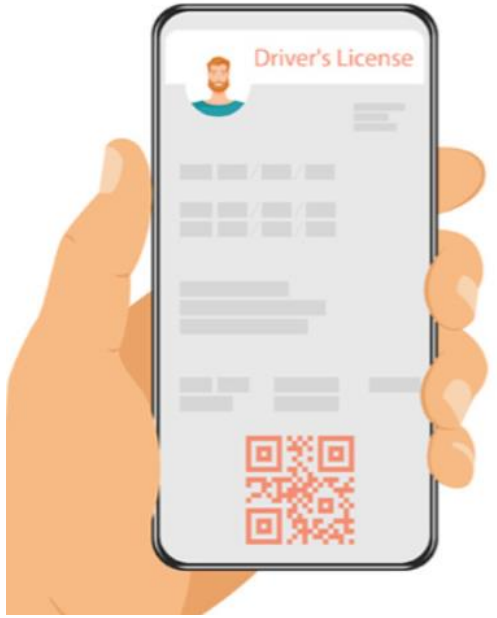
- Government issued vaccination certification service, named COOV (Corona Overcome), from this April 2021
- Blockchain and decentralized identity (DID) technology are used to prevent the possibility of forgery or alteration.
- KCDA only records information that can verify data's authenticity.
- Individuals can personally manage personal information such as resident registration numbers and directly decide whether to disclose additional information such as name, date of birth, nationality, and passport number.
- Mutual recognition will be sought with other countries or regions.

Korea Disease Control and Prevention Agency

(Source: https://www.koreabiomed.com/news/articleView.html?idxno=10937)

A use case - decentralized identity for mobile driver's licenses in Korea

- A mobile driver's license that uses decentralized identity (DID) technology.
- A digital national identity credential based on a driver's license issued by the National Police Agency.
- Equivalent to the existing plastic driver's licenses and plans to launch by year 2021's end.
- First national identity based on DID technology and blockchain.
- Operated by Ministry of the Interior and Safety.

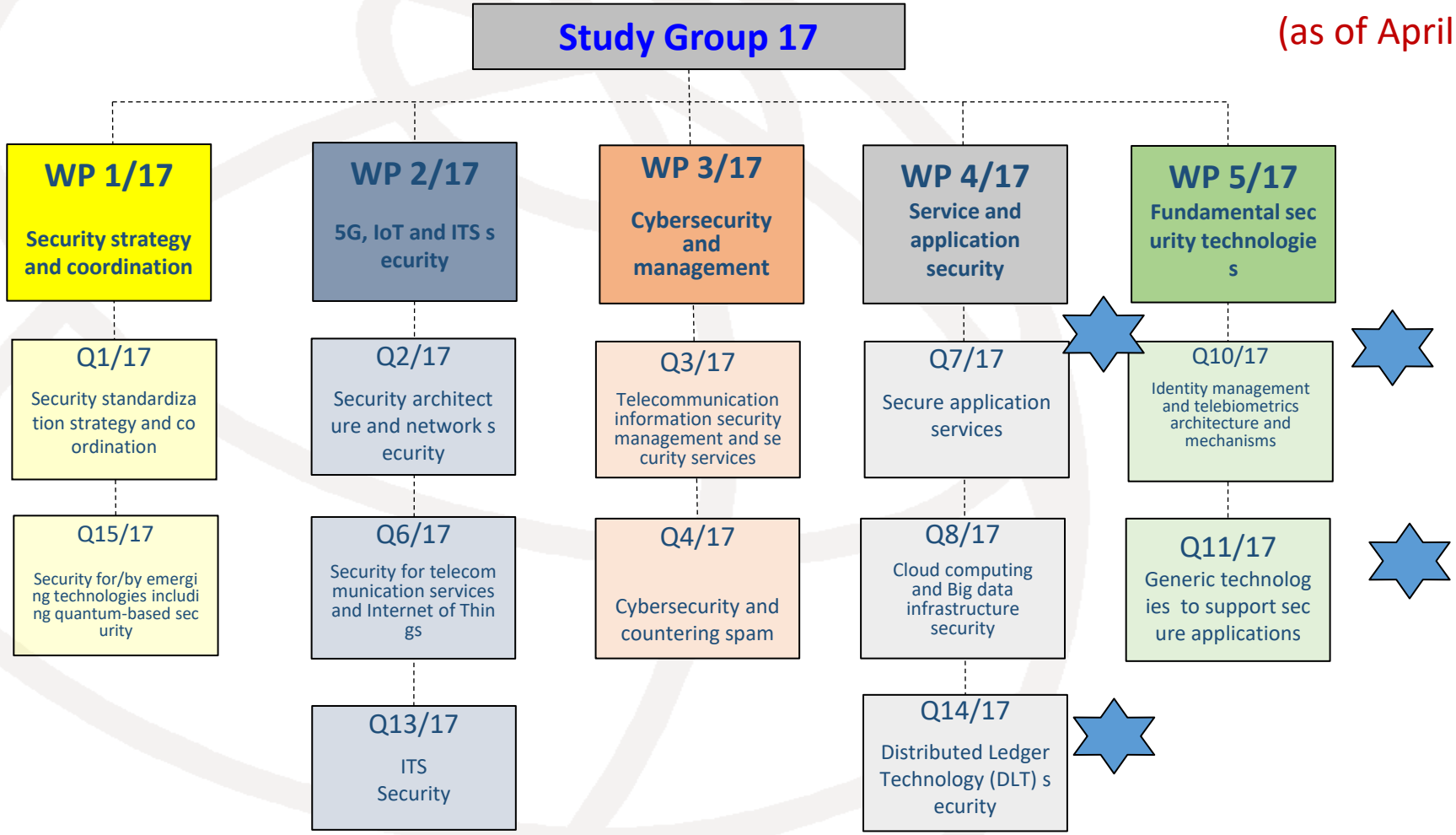


Ministry of the Interior and Safety

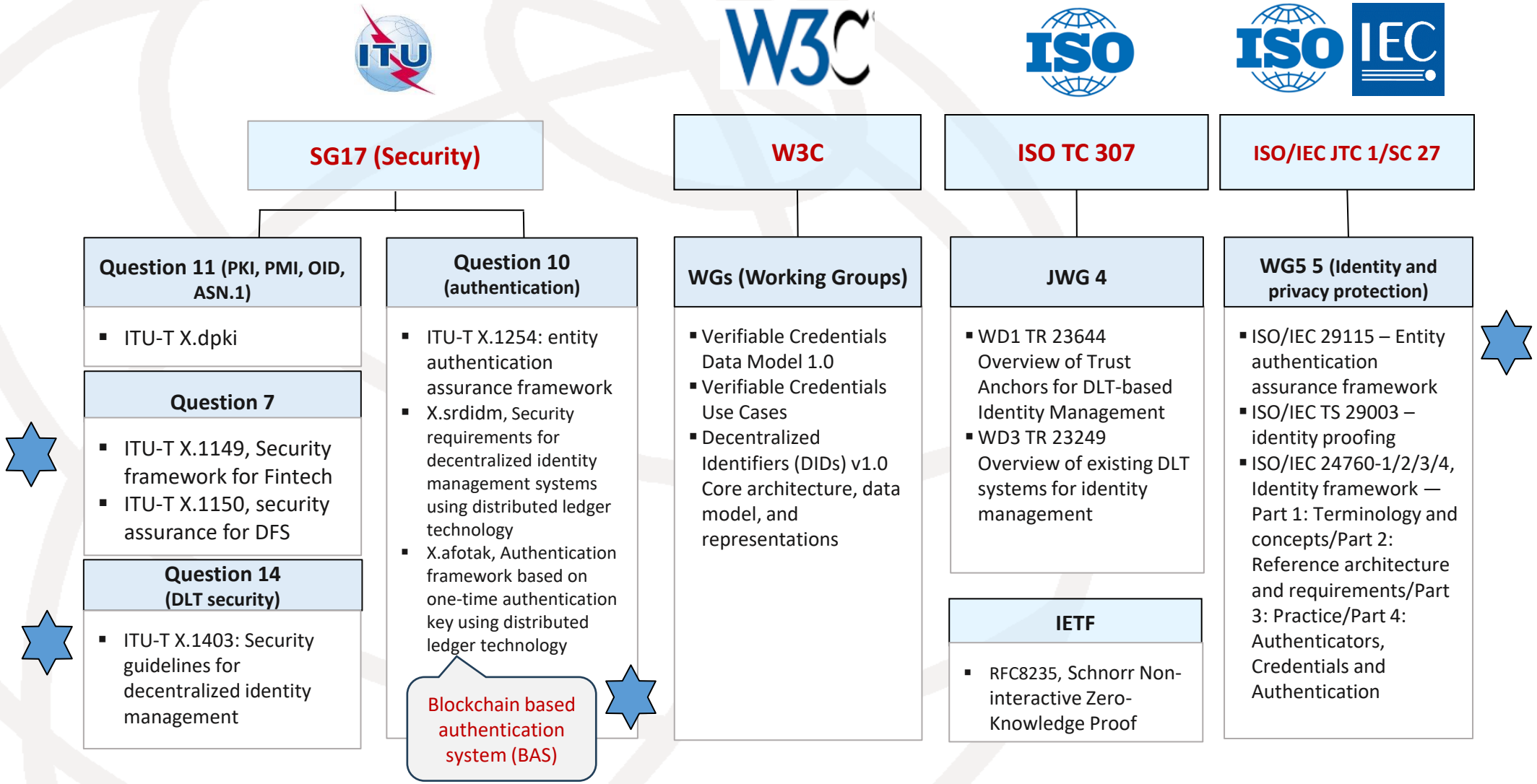
(Source: https://www.ledgerinsights.com/lg-cns-korean-decentralized-identity-did-for-drivers-licenses/)

Structure of ITU-T SG17, Security

(as of April 2024)



Global SDOs working on authentication and decentralized Identity



Concluding remark

- Four key security measures are implemented to ensure security for Fintech services.
- Providing security assurance for Fintech services is critical (please see details in ITU-T X.1150 and X.1149).
- Two aspects for security (i.e., ITU-T X.1149) and privacy (i.e., ISO/IEC 27562) of Fintech services needs to be applied.
- Decentralized identity should be utilized for strong identity and self-control of identity in Fintech services.

Thank you for your attention.