Introduction to ISO 27565

Information security, cybersecurity and privacy protection —

Guidelines on Privacy Preservation based on Zero Knowledge Proofs

Bingsheng Zhang

Zhejiang University, China

Outline

01

Background

02

Scope & Status

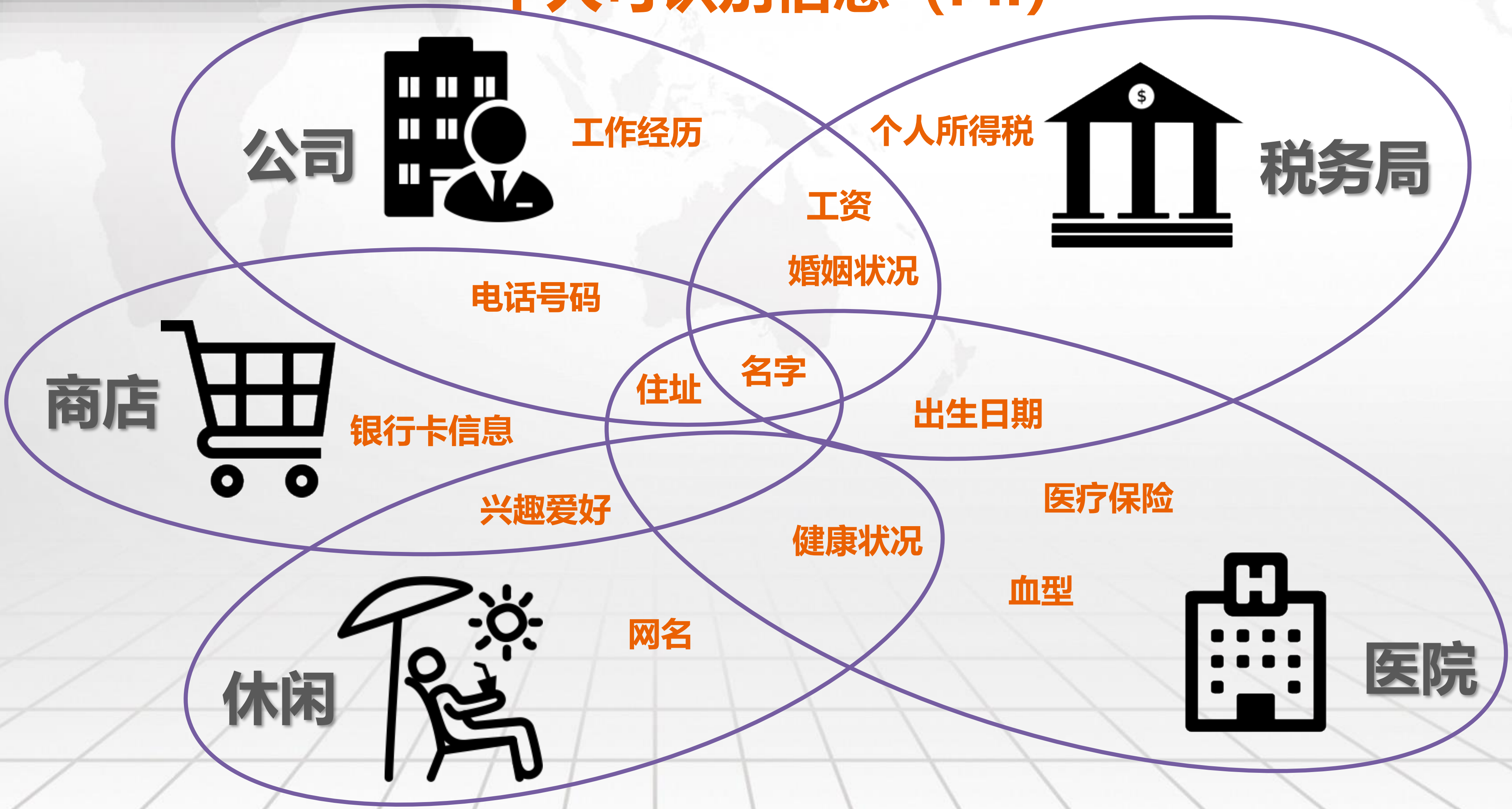
03

Contents

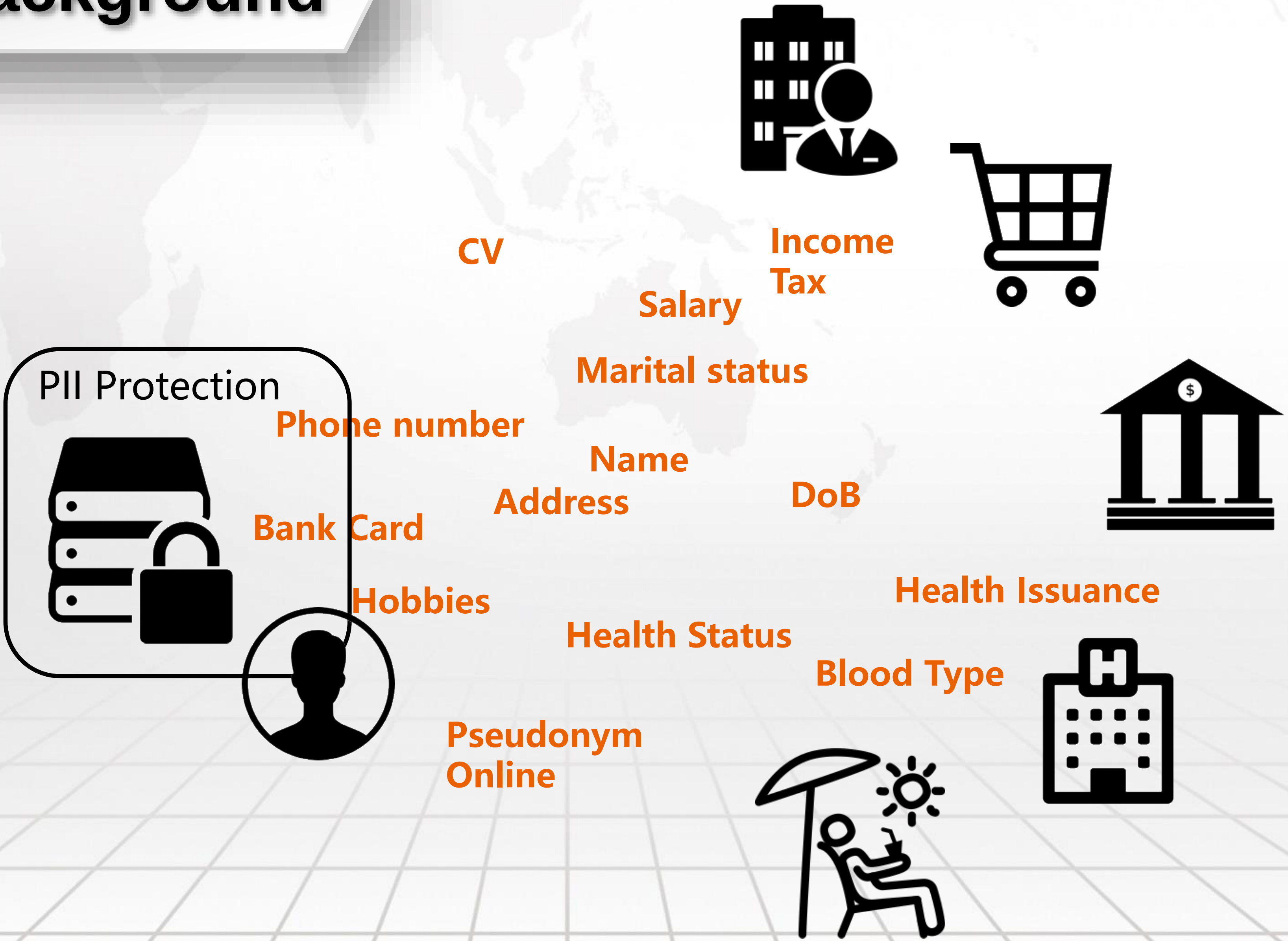
Background

Background

个人可识别信息（PII）



Background



PII Protection

CV

Income Tax

Salary

Marital status

Phone number

Name

Address

DoB

Bank Card

Hobbies

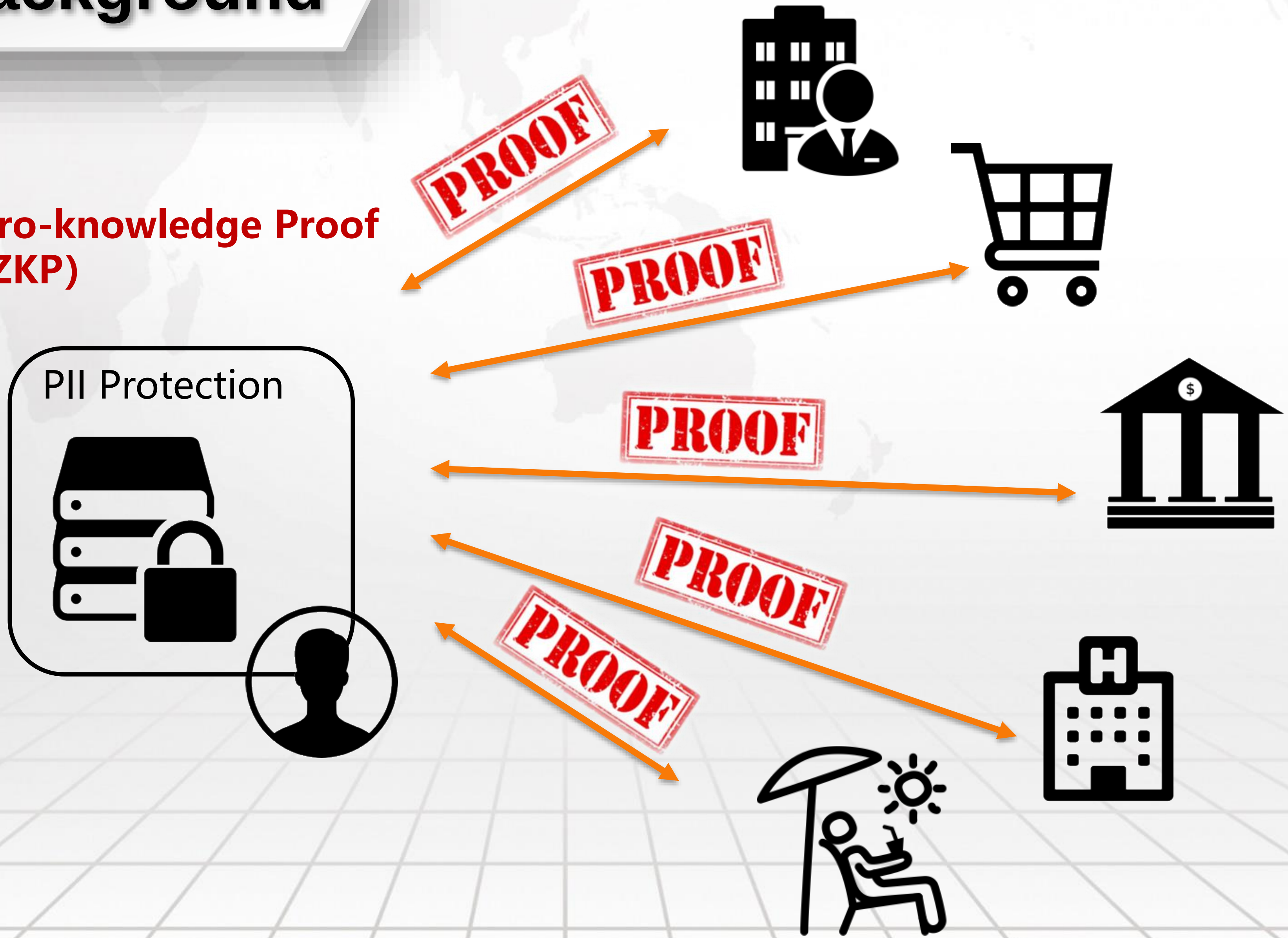
Health Issuance

Health Status

Blood Type

Pseudonym Online

Background



Zero-knowledge Proof (ZKP)

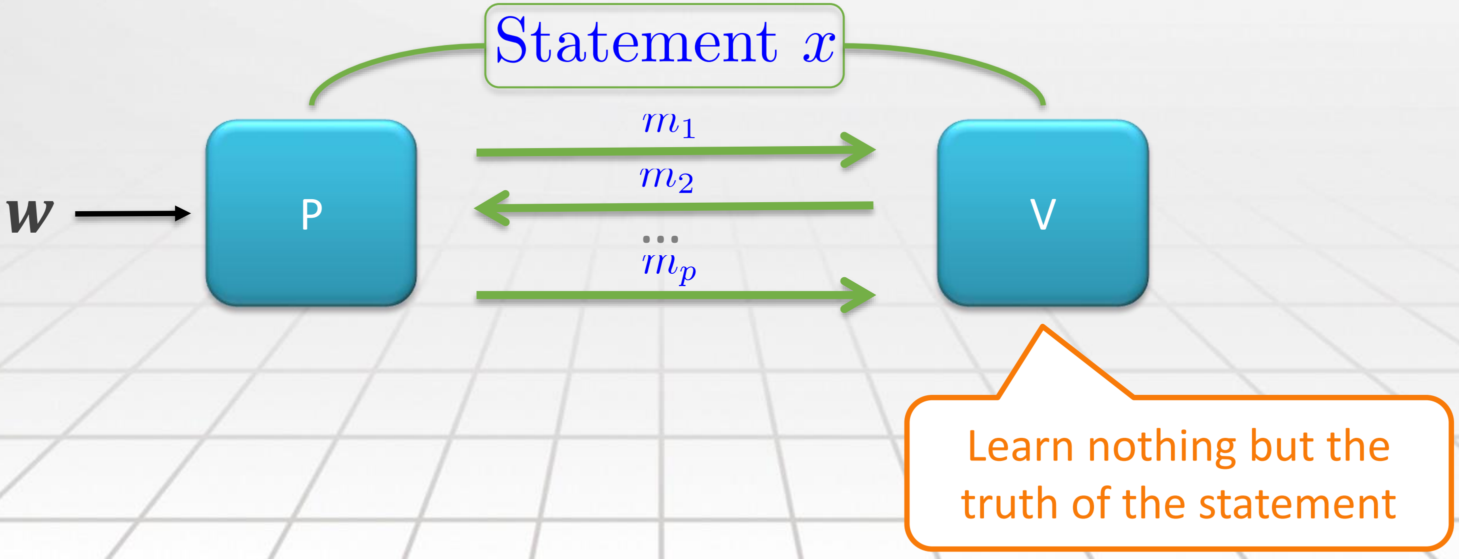
PII Protection

What is a ZKP?

What is a zero-knowledge proof （ZKP）？

Let $\mathcal{R}_L$ be a witness relation associated with $L \in \mathcal{NP}$

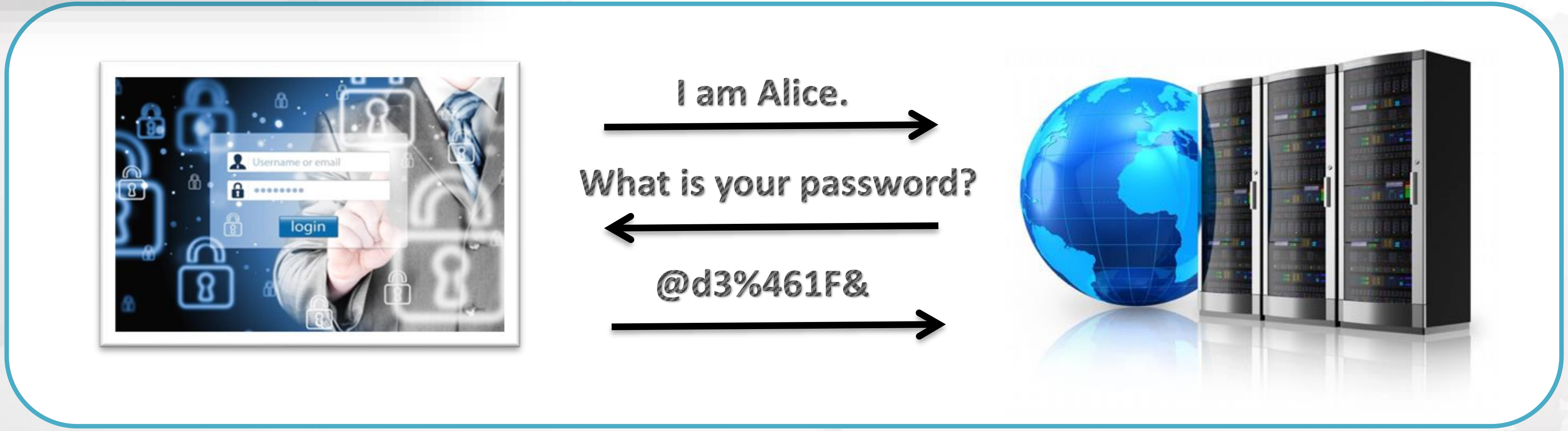
$$L = \{x : \exists w \text{ s.t. } (x, w) \in \mathcal{R}_L\}$$



Learn nothing but the truth of the statement

Example

Now

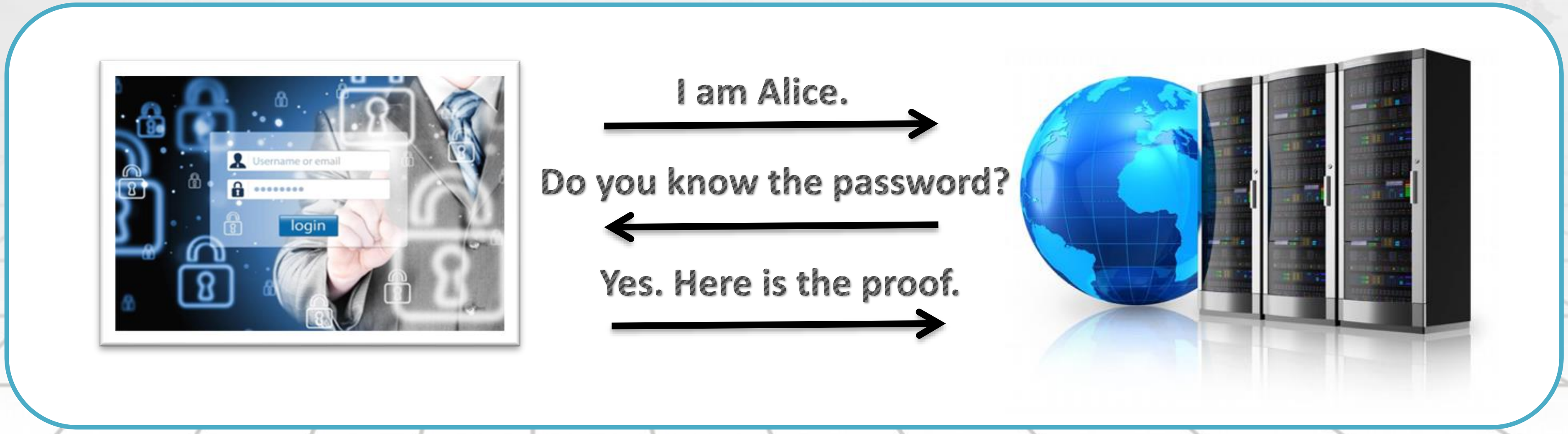


I am Alice.

What is your password?

@d3%461F&

Vision



I am Alice.

Do you know the password?

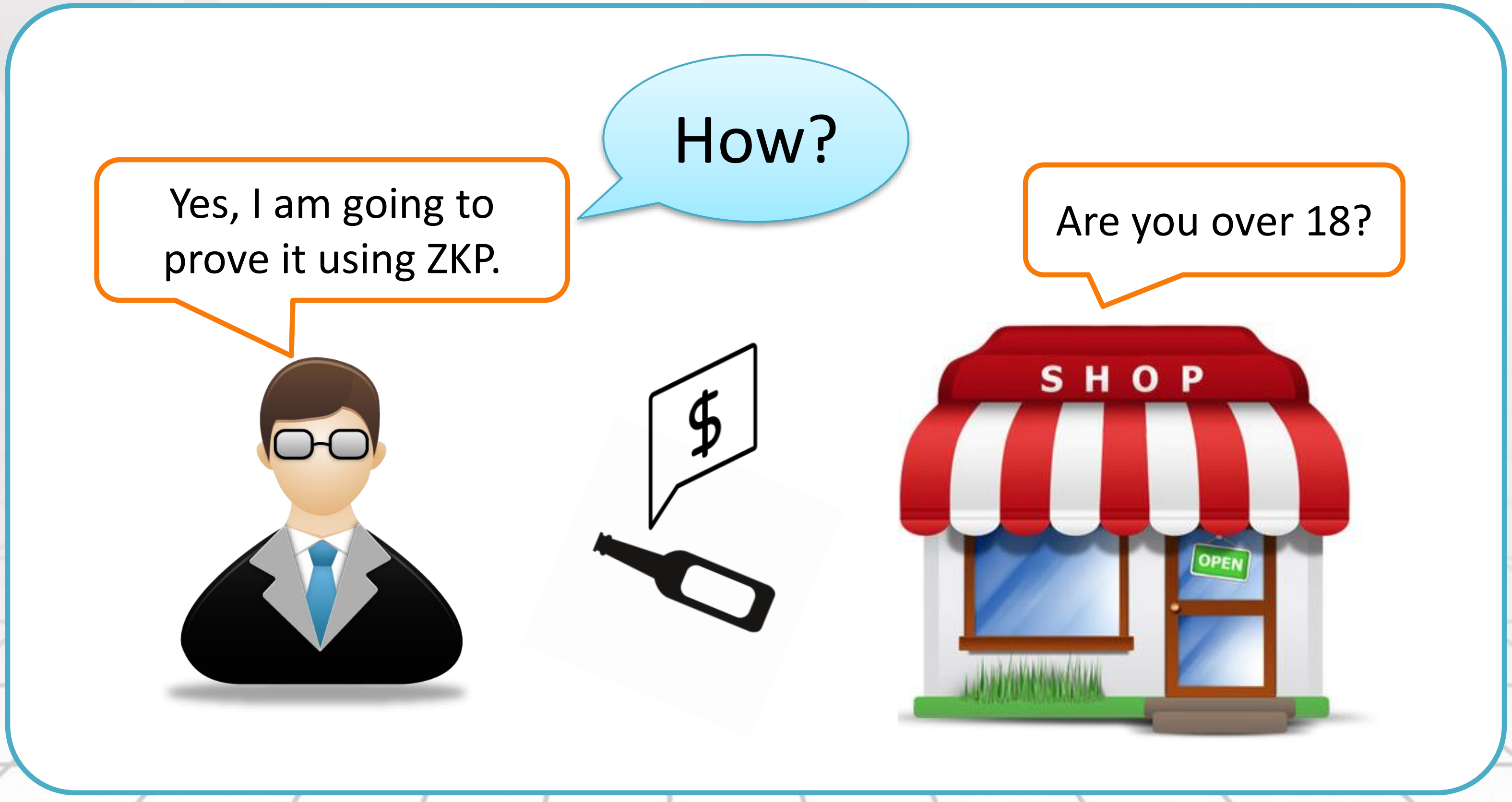
Yes. Here is the proof.

Scope & Status

Why 27565 is needed?

It is not easy to use ZKP right !

ZKP can prove a number is larger than 18, then what?



Why 27565 is needed?

- Problem statement：
  - ZKP can only prove a digital assert holds certain property.
  - How to link real-world with digital world?
    - e.g. why the number represents your age or your salary, etc.

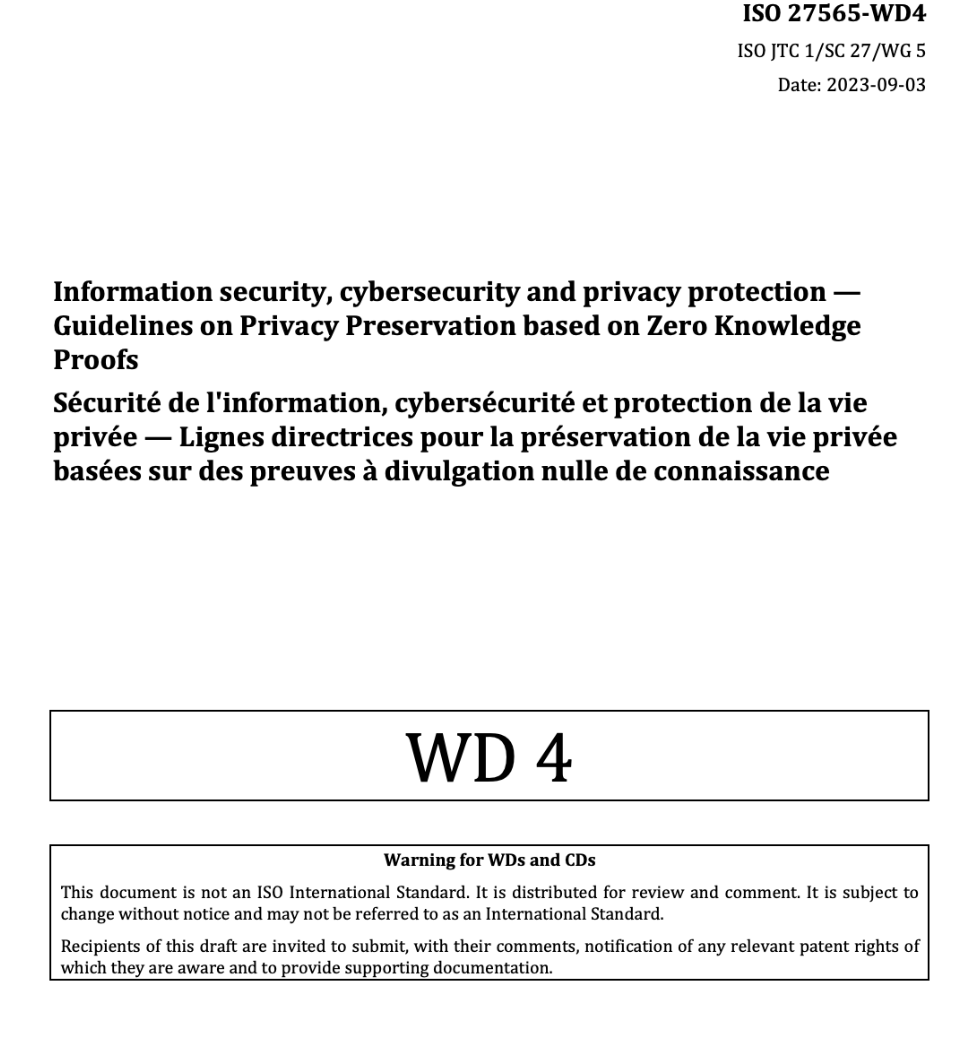
- ISO 27565：
  - Provide a framework on how to use ZKP for PII protection in practice.

Scope

This document provides guidelines on using zero-knowledge proofs (ZKP) to improve privacy by reducing the risks associated with the sharing or transmission of personal data between organisations and users by minimizing unnecessary information disclosure.

It includes several ZKP functional requirements relevant to a range of different business use cases, then describes how different ZKP models can be used to meet those functional requirements securely.

Status



ISO 27565-WD4

ISO JTC 1/SC 27/WG 5

Date: 2023-09-03

Information security, cybersecurity and privacy protection — Guidelines on Privacy Preservation based on Zero Knowledge Proofs

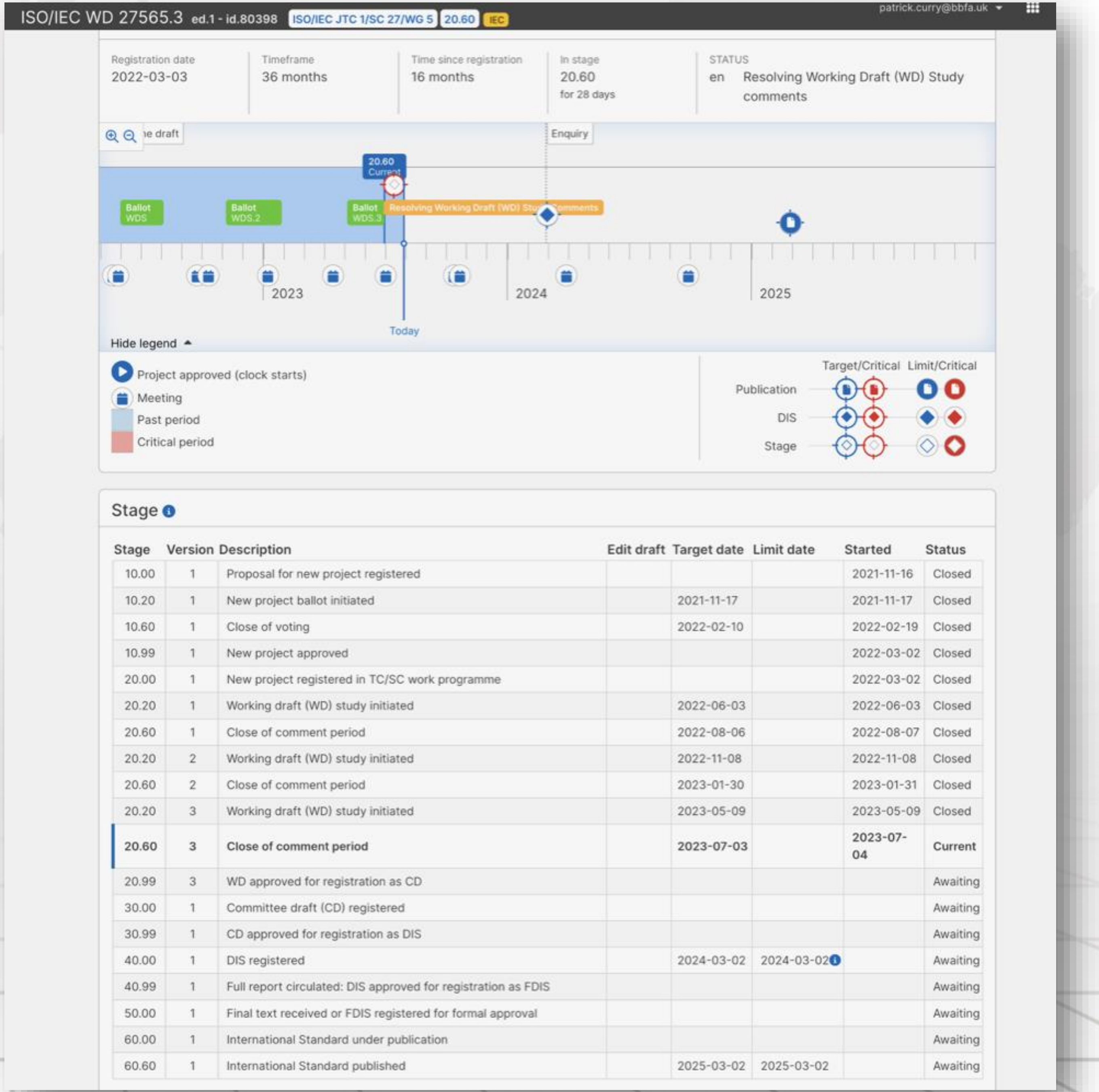
Sécurité de l'information, cybersécurité et protection de la vie privée — Lignes directrices pour la préservation de la vie privée basées sur des preuves à divulgation nulle de connaissance

WD 4

Warning for WDs and CDs

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.



ISO/IEC WD 27565.3 ed.1 - id.80398 ISO/IEC JTC 1/SC 27/WG 5 20.60 IEC

patrick.curry@bbfa.uk

Registration date: 2022-03-03

Timeframe: 36 months

Time since registration: 16 months

In stage: 20.60 for 28 days

STATUS: en Resolving Working Draft (WD) Study comments

Stage

Stage	Version	Description	Edit draft	Target date	Limit date	Started	Status
10.00	1	Proposal for new project registered				2021-11-16	Closed
10.20	1	New project ballot initiated		2021-11-17		2021-11-17	Closed
10.60	1	Close of voting		2022-02-10		2022-02-19	Closed
10.99	1	New project approved				2022-03-02	Closed
20.00	1	New project registered in TC/SC work programme				2022-03-02	Closed
20.20	1	Working draft (WD) study initiated		2022-06-03		2022-06-03	Closed
20.60	1	Close of comment period		2022-08-06		2022-08-07	Closed
20.20	2	Working draft (WD) study initiated		2022-11-08		2022-11-08	Closed
20.60	2	Close of comment period		2023-01-30		2023-01-31	Closed
20.20	3	Working draft (WD) study initiated		2023-05-09		2023-05-09	Closed
20.60	**3**	**Close of comment period**		**2023-07-03**		**2023-07-04**	**Current**
20.99	3	WD approved for registration as CD					Awaiting
30.00	1	Committee draft (CD) registered					Awaiting
30.99	1	CD approved for registration as DIS					Awaiting
40.00	1	DIS registered		2024-03-02	2024-03-02		Awaiting
40.99	1	Full report circulated: DIS approved for registration as FDIS					Awaiting
50.00	1	Final text received or FDIS registered for formal approval					Awaiting
60.00	1	International Standard under publication					Awaiting
60.60	1	International Standard published		2025-03-02	2025-03-02		Awaiting

Document Structure

1. Scope
2. Normative references
3. Terms and definitions
4. Abbreviated terms
5. Introduction to Zero-knowledge Proofs
6. Architectural Options for ZKP
7. Applications of ZKP for Privacy Preservation
8. Privacy Considerations
9. Privacy Risk Assessment
10. Security Considerations

Contents

Intro to ZKP

A ZKP makes it possible to prove that a statement or a set of statements is true while preserving confidentiality of secret information. This makes sense when the veracity of the statement or a set of statements is not obvious on its own, but the prover knows relevant secret information that enables a proof to be made.

A ZKP protocol must support the following three properties: completeness, soundness and zero-knowledge:

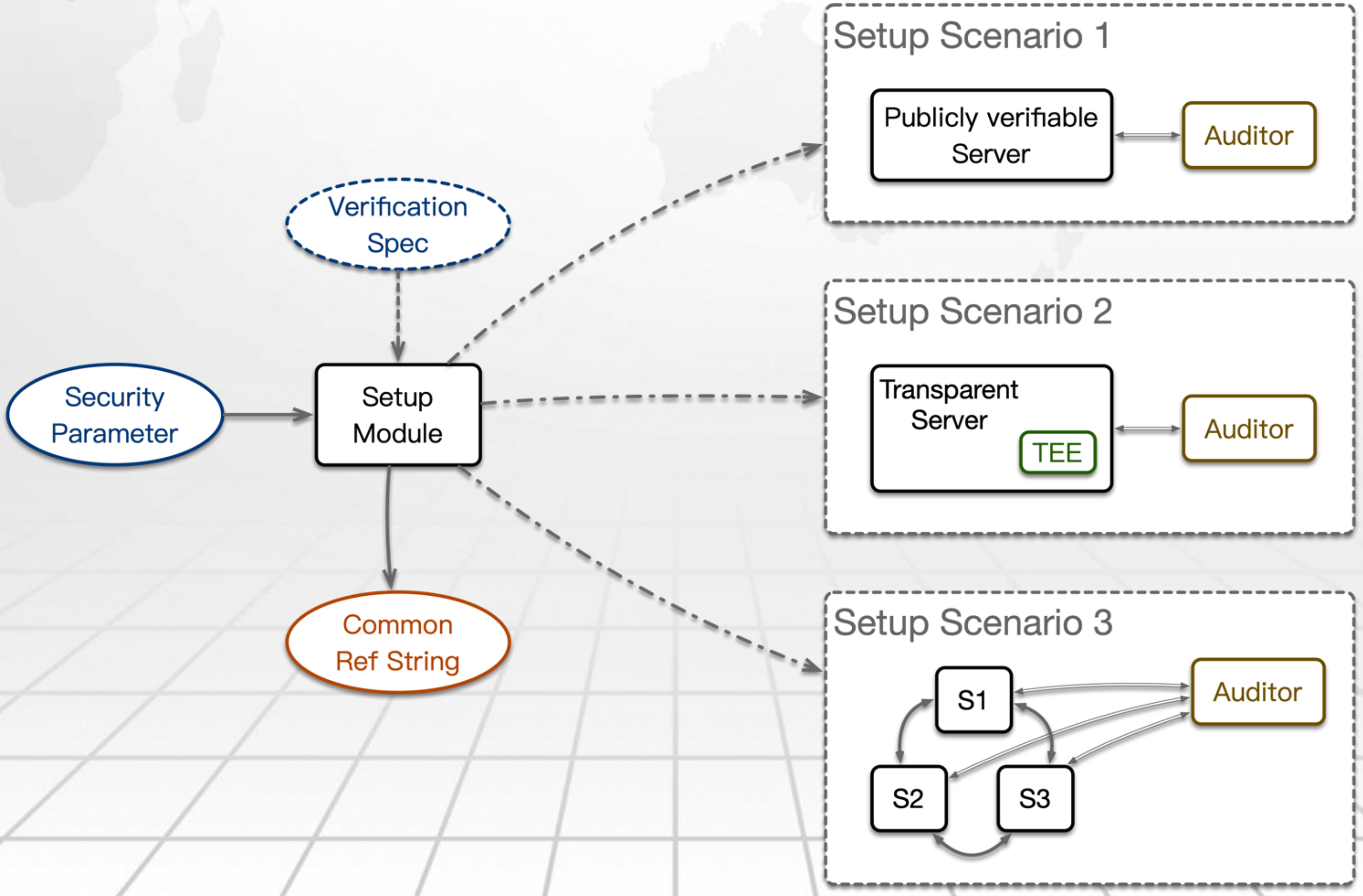
- completeness: If the prover's statement is true, then the verifier will accept it with overwhelming probability.
- soundness: If the prover's statement is false, then no matter how the prover behaves, the verifier will reject it with overwhelming probability.
- zero-knowledge: if the statement is true, no verifier learns any information other than the fact that the statement is true.

Architectural Options

- Interactive zero-knowledge proofs
  - Sigma protocol
- Non-interactive zero-knowledge proofs
  - Using hash to simulate the verifier's actions
  - Using trusted public source of randomness to simulate the verifier's actions
  - Using a structured common reference string (CRS)
- Attribute providers
  - Attributes related to the prover are typically held by some trusted third parties, e.g. a bank. They can disclose a subset of the attributes they hold or can generate computed attributes from them, for example by computing the age of a person by making a subtraction between the current date and the date of birth of the person.

Architectural Options

- Components of a ZKP system
  - Setup module



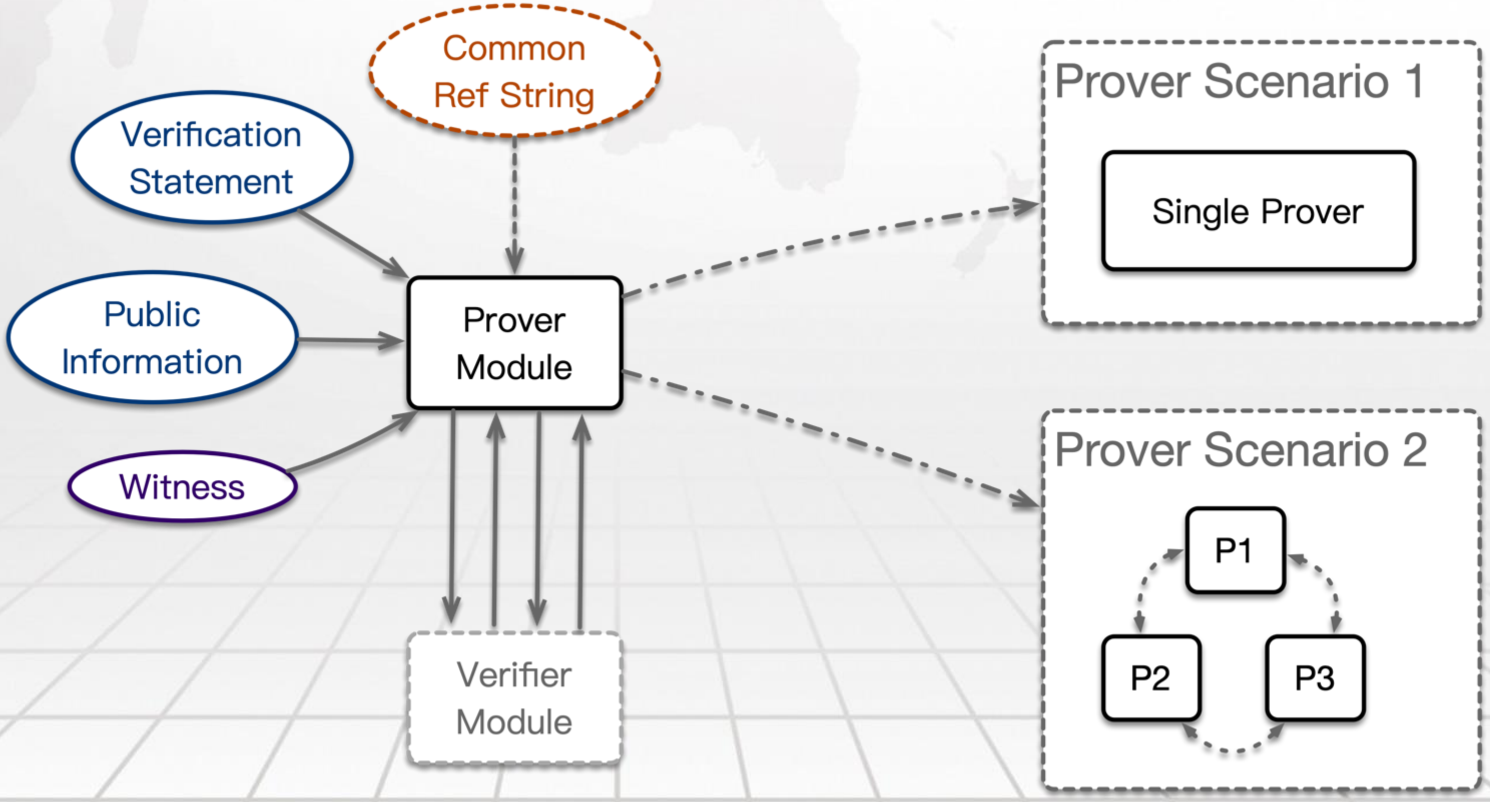
Architectural Options

- Components of a ZKP system
  - Setup module

  - There are several variations of the setup and the level of trust placed in it
    - No setup or trustless setup
    - Uniform random string
    - Common reference string
    - Designated verifier setup
    - Random oracle model
    - Updatable CRS

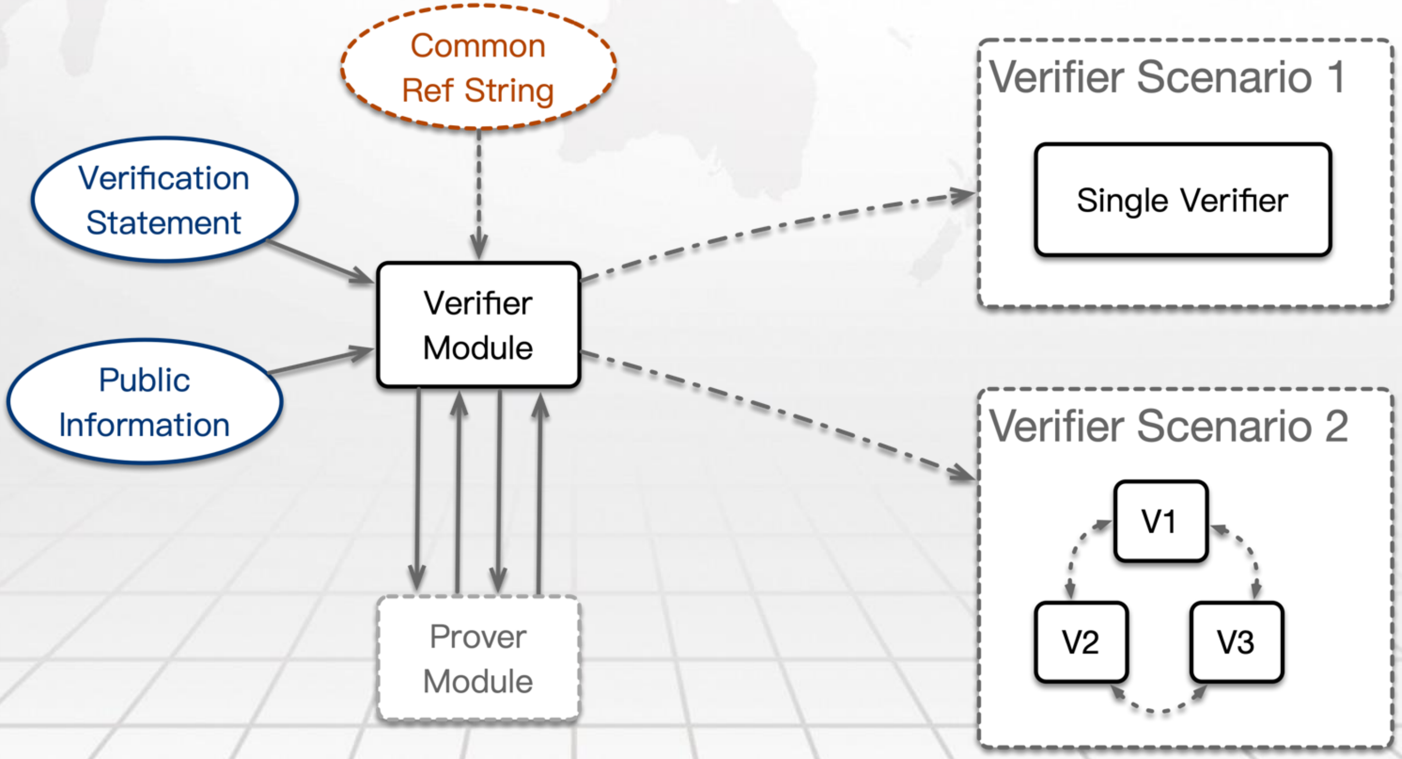
Architectural Options

- Components of a ZKP system
  - Prover module



Architectural Options

- Components of a ZKP system
  - Verifier module



Architectural Options

- Subject binding
  - To associate a statement with the right individual, either a user identifier or one or more identifying attributes that relates to the individual need to be included into the common knowledge statement. The user identifier or the identifying attribute(s) should be sufficient, within a given context, to uniquely relate to the user. Such information is called a distinguishing identifier.
  - The attribute provider must verify that the value placed in the user identifier or/and in one or more identifying attributes indeed correspond to attributes that belong to the correct user.

Architectural Options

- Subject binding
  - A user identifier may be either:
    1. a globally unique user identifier, or
    2. a locally unique user identifier used to identify a user whatever verifier is being involved,
    3. a unique user identifier used to identify a user for each attribute providers / verifier pair, or
    4. a unique user identifier used to identify a user for each user/ verifier pair, or
    5. a temporary user identifier.

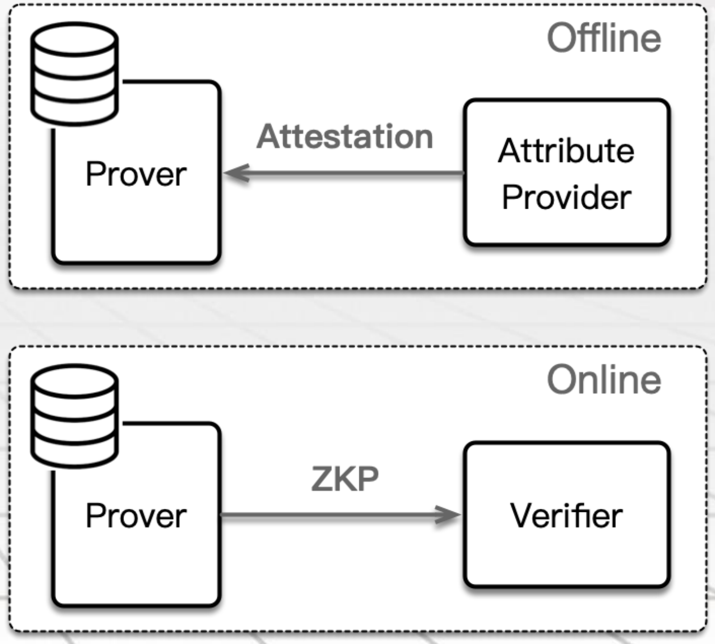
Architectural Options

- Characteristics of ZKPs
  - ZKP applied to the content of one authoritative document
  - ZKP applied to the content of several authoritative documents
  - Replay detection or protection
  - ZKP performance
  - ZKP Interoperability

Architectural Options

- Selective disclosure of attributes
  - Individuals may be provided with various forms of attestations issued, e.g., by governmental agencies, social security agencies, insurance companies, banks, schools or universities, ... that often contain more information than strictly necessary to be disclosed to a verifier.

  - Pre-generation of attestations
  - On-demand generation of attestations
  - Proving some properties of a hidden attribute



Applications of ZKP

- Functional Use Cases
  - Age Verification
  - Fraud Prevention
  - Auction
  - Distributed Ledger Technologies (DLT) and blockchains
  - Central Bank Digital Currencies (CBDCs)

Privacy considerations

- Data minimization
- Consent and choice
- Purpose legitimacy and specification
- Collection limitation
- Anonymity of the authority that has issued the attestation
- Non-disclosure of the identity of the verifiers to the attribute issuer
- Use, retention and disclosure limitation
- Accuracy and quality
- Openness, transparency and notice
- Individual participation and access
- Accountability
- Information security
- Privacy compliance
- Unlinkability

Privacy Risk Assessment

- The privacy impact assessment must consider all potential privacy threats associated with the use case and the context. Some of the threats pertaining that get minimized or eliminated by use of ZKP are:
  - Collection of Identity information, when such identity is desirable but not essential in delivering the service, e.g., when an ID card is used to verify age
  - Knowledge of personal information about the individual that is not needed but could have adverse consequences, e.g., when a passport is checked to ascertain eligibility to travel, an individual's address and country that issued a visa is also known. Likewise, a participants' bid information is known in an auction;
  - Linkability and consequent misuse of personal data, e.g., when identity is known along with travel history;
  - Risk of data leakage or unauthorised access is eliminated by not collecting information or capturing only minimal information.

Security Considerations

- Alice and Bob collusion attack
  - Prevention of collusions between users
- Use of an authoritative document or of a trusted authority

- Annex
  - Factors hindering and facilitating ZKP developments
  - An example of a consistency check between two documents
  - An example of selective disclosure
  - An example of secure comparison of two numbers

Email: bingsheng@zju.edu.cn