Conformity assessment and standards

CIS 2017, June 22, 2017

Andrew Hughes, CISM CISSP
Leadership Council Chair, Kantara Initiative

KantaraInitiative.org

© Copyright 2017 Kantara Initiative, Inc.

TODAY'S TOPICS

- The elements of Conformity Assessment Systems
- Use of standards and conformity assessment to evaluate **promised** services as **'fit for purpose**' and '**meets expectations**'
- Principles and Value of Open Standards

© Copyright 2017 Kantara Initiative, Inc.

Problem: Gaining Trust in Promised Services

- What do you & your organization look for in online products and services to believe they are trust-worthy and are a solid solution?
- How can a commercial reputation for quality be expressed?
- Is this a hard problem to solve?

© Copyright 2017 Kantara Initiative, Inc.

Some Possible Solutions

- Use recognized standards to develop and deliver services
- Undergo conformity assessment and obtain a licensed Mark of conformity as evidence of conforming to specified standards
- Negotiate contracts (unilateral, bi-lateral, multi-lateral)
- Purchase services that display the desired Mark of conformity

© Copyright 2017 Kantara Initiative, Inc.

Some Concepts

- **Standards** are a consensus on how an activity *should be done* or a product made. They should be developed using open, transparent, voluntary processes

- **A Mark of Conformity** represents a *commitment* by the licensee to achieve specified quality as defined in a standard

- **Conformity Assessment** is used to evaluate how an activity *is actually being done* (and may result in issuance of a licensed Mark)

© Copyright 2017 Kantara Initiative, Inc.

A Scenario

SHOEME.COM AND PERSONAL DATA PROTECTION RISKS

© Copyright 2017 Kantara Initiative, Inc.

THE SCENARIO

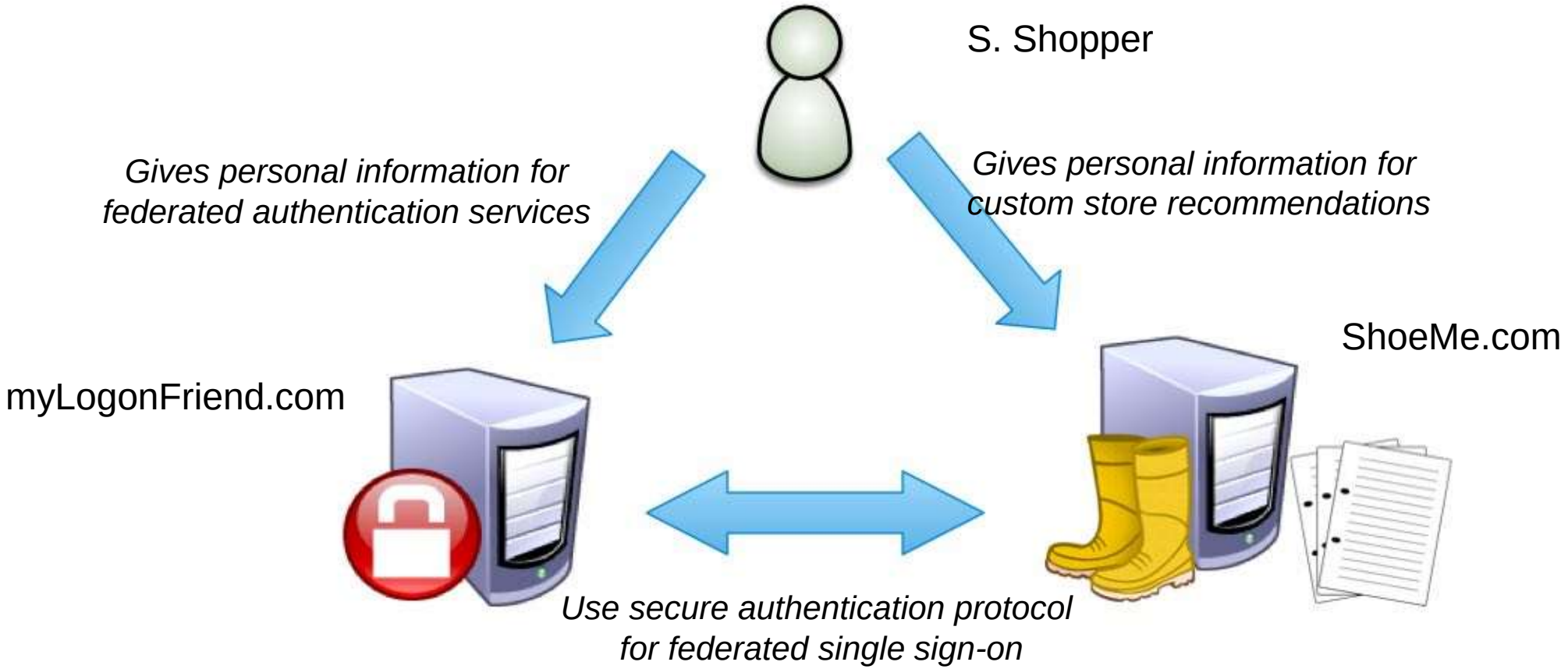
- Overall scenario – online retail based on personal information and preferences
- Problem – each participant is at risk if the other is a bad apple or careless
- Solution – What do you do in real life?
  - get information about track record
  - determine if good practices are used
- How is this possible in the online world?

© Copyright 2017 Kantara Initiative, Inc.

SCENARIO – SHOEME.COM

© Copyright 2017 Kantara Initiative, Inc.

SCENARIO – SHOEME.COM

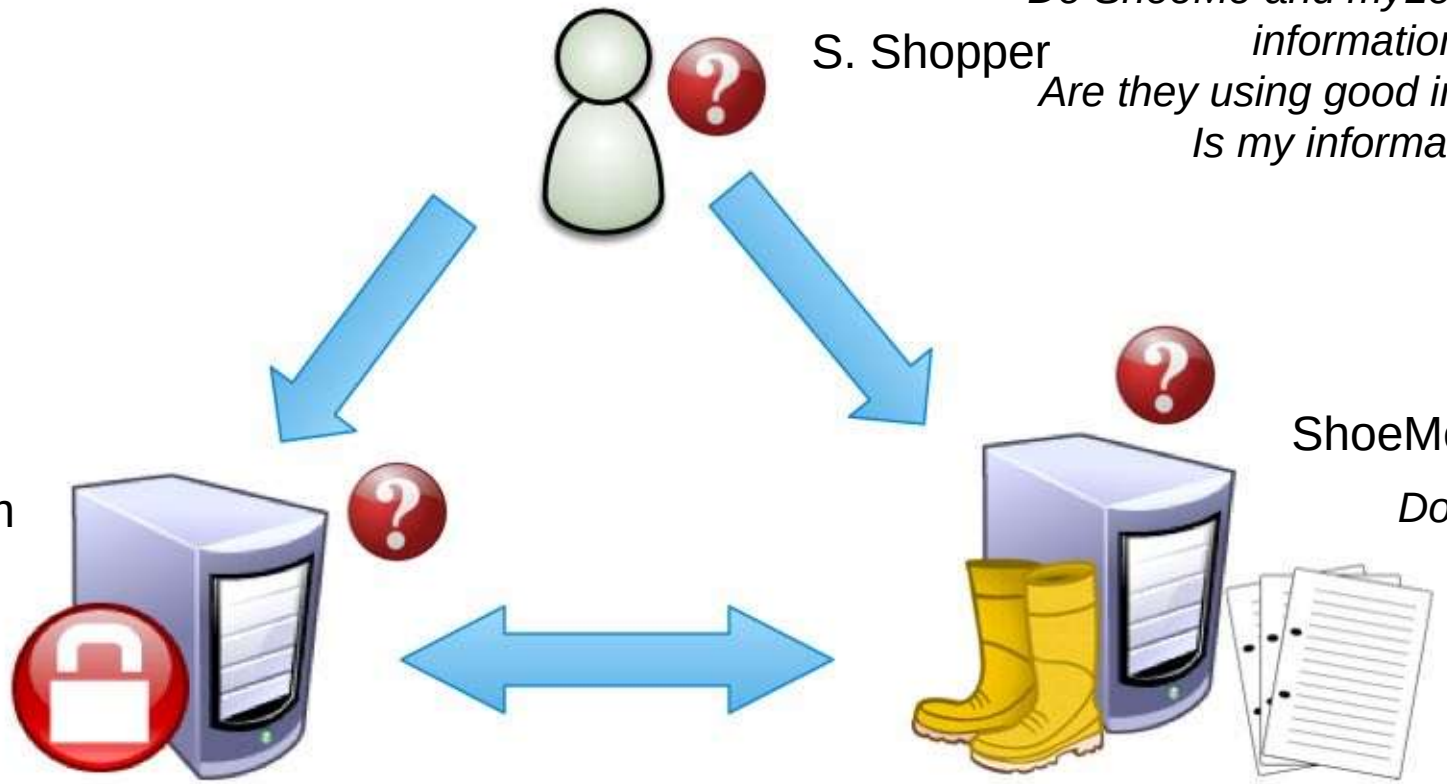


© Copyright 2017 Kantara Initiative, Inc.

SCENARIO – SHOEME.COM

S. Shopper

Do ShoeMe and myLogonFriend protect information well?
Are they using good industry practices?
Is my information safe?



myLogonFriend.com

Does ShoeMe protect information well?
Do they comply with regulations?

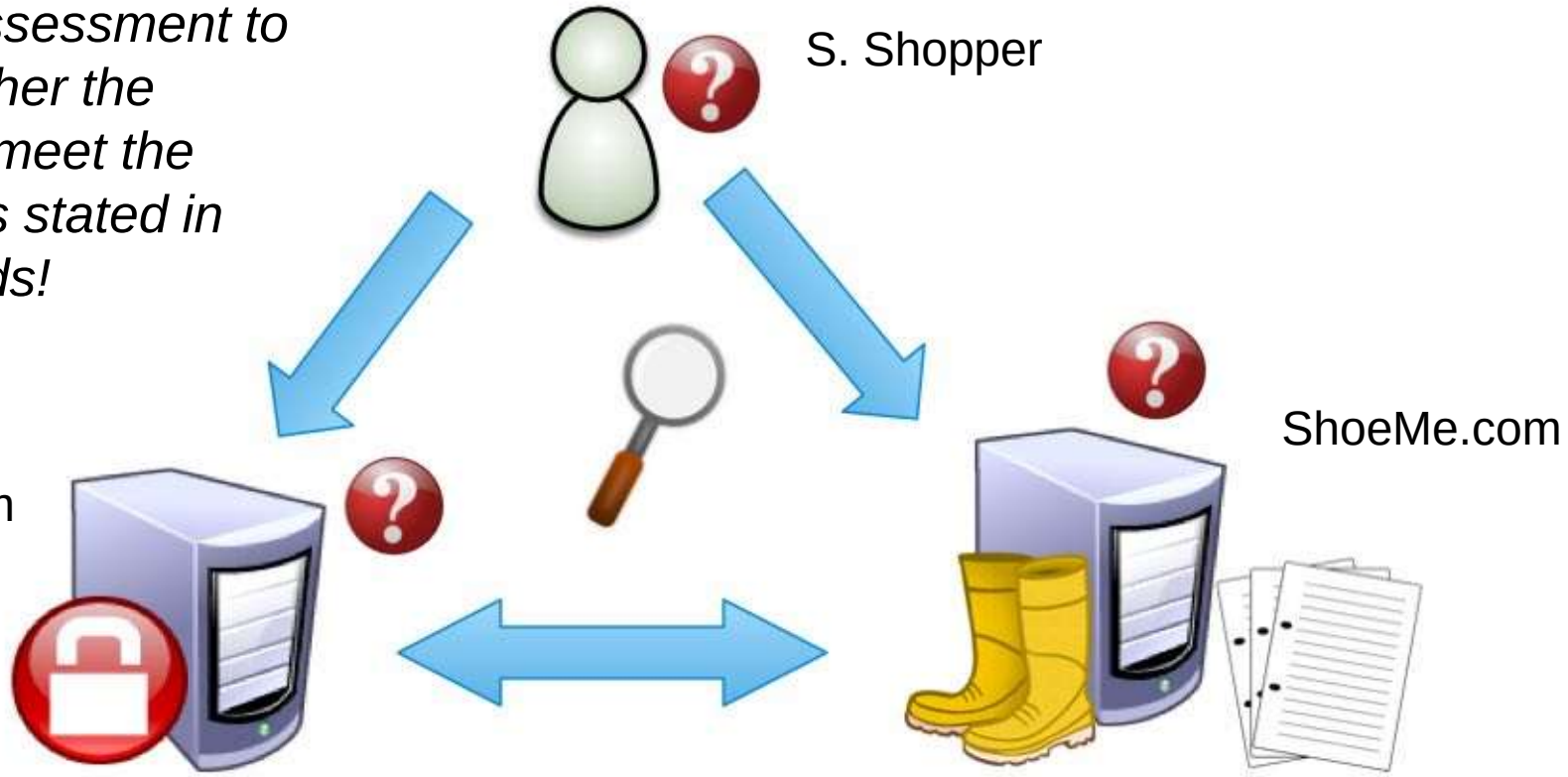
ShoeMe.com

Does myLogonFriend protec information well?
Do they comply with regulations?

© Copyright 2017 Kantara Initiative, Inc.

SCENARIO – SHOEME.COM

Use Conformity Assessment to assess whether the organizations meet the requirements as stated in standards!



© Copyright 2017 Kantara Initiative, Inc.

CONFORMITY ASSESSMENT

© Copyright 2017 Kantara Initiative, Inc.

Definition: Conformity Assessment

- Conformity assessment: *demonstration* that *specified requirements* relating to a product, process, system, person or body are *fulfilled*
(ISO/IEC 17000:2004)

© Copyright 2017 Kantara Initiative, Inc.

The Value of Conformity Assessment

- Undergoing the conformity assessment process has a number of benefits:
  - It provides consumers and other stakeholders with added confidence.
  - It can give your company a competitive edge.
  - It helps regulators ensure that health, safety, environmental conditions, security and other requirements are met.

© Copyright 2017 Kantara Initiative, Inc.

ISO/IEC 17000 'Functional Approach'

- ISO/IEC 17000
  Conformity assessment – Vocabulary and general principles
  - Part of a family of standards on Conformity Assessment
  - 'Functional Approach' is proposed
    - *Selection* – choose the standard; decide on sampling & techniques
    - *Determination* – testing, inspection, auditing, examination
    - *Review & Attestation* – decide on conformity to the specified requirements; issue statement of conformity; issue a Mark
    - *Surveillance* – monitoring out in the marketplace

© Copyright 2017 Kantara Initiative, Inc.

WHAT IS A MARK OF CONFORMITY?

© Copyright 2017 Kantara Initiative, Inc.

Mark of Conformity

- A Mark of conformity is an indication that an organization has demonstrated conformity to standards which set expectations of quality.
- A Mark of conformity may be licensed to qualified organizations.
- The license contains terms and conditions to have the right to use the mark – e.g. the licensee must remain in conformity

© Copyright 2017 Kantara Initiative, Inc.

Why Trust A Mark Issuer?

- A Mark issuer conforms to standards (of course).
  The issuer uses a formal conformity assessment system to ensure the quality of the licensee's products and services

- Mark issuers should be Accredited: evaluated by peers to confirm quality of the conformity assessment scheme and Mark license

- Accreditation increases the value of issued Marks

© Copyright 2017 Kantara Initiative, Inc.

CONFORMITY ASSESSMENT SYSTEM

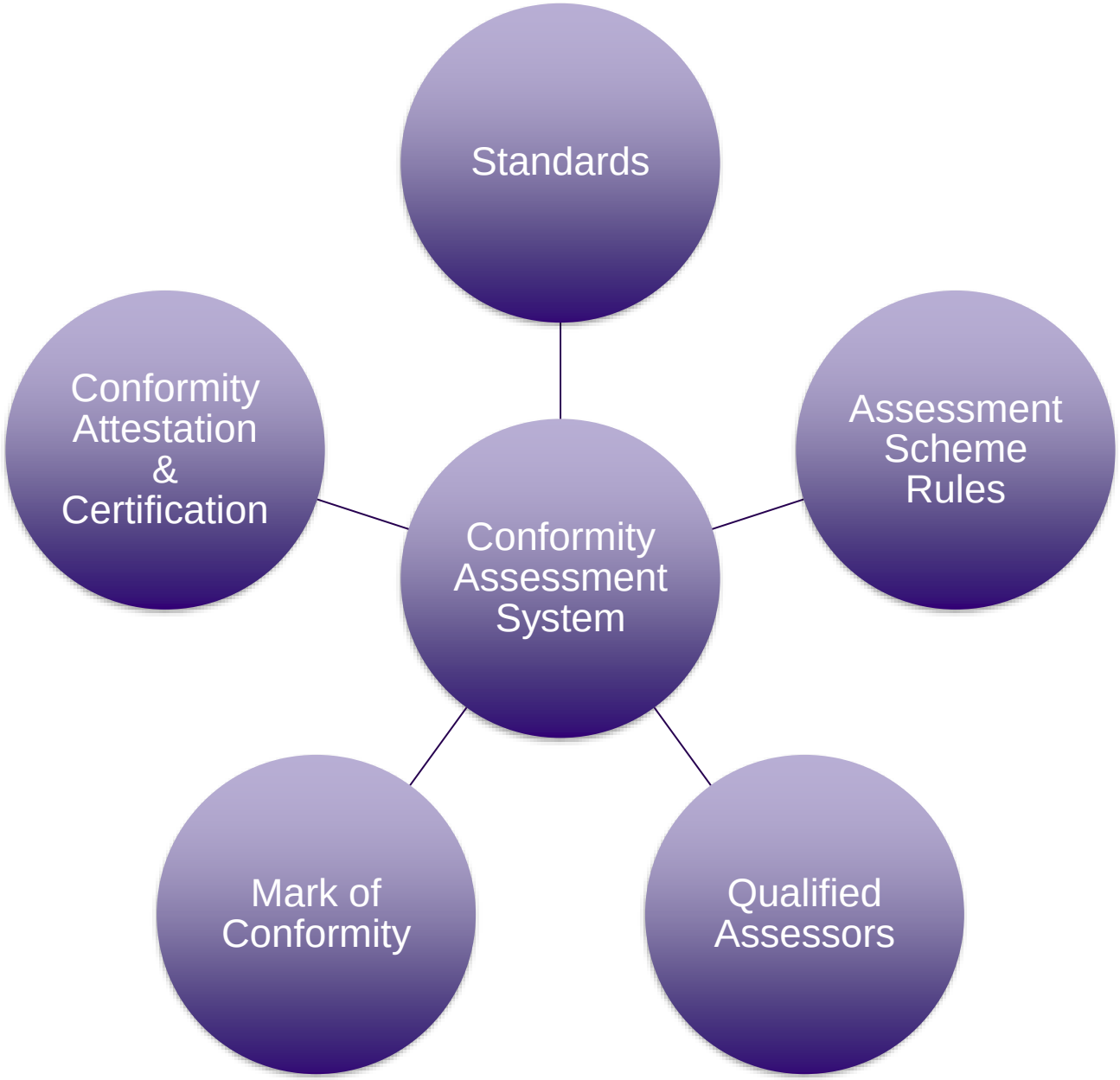
© Copyright 2017 Kantara Initiative, Inc.

What is a System of Conformity Assessment?

- Conformity assessment system: rules, procedures and management for carrying out conformity assessment
(ISO/IEC 17000:2004)

© Copyright 2017 Kantara Initiative, Inc.

Conformity Assessment System



© Copyright 2017 Kantara Initiative, Inc.

Who Performs Assessments?

- 1st Party Assessment = Internal Independent Assessor
- 2nd Party Assessment = A Supplier requirement
- 3rd Party Assessment = External Independent Assessor

- Significance
  - There is high value in each type of conformity assessment; 3rd party assessment (certification) is not always required

© Copyright 2017 Kantara Initiative, Inc.

Examples of

CONFORMITY ASSESSMENT SCHEMES

© Copyright 2017 Kantara Initiative, Inc.

An Identity Assurance Assessment Scheme

- The Kantara Identity Assurance Assessment Framework
  - Assess fulfilment of requirements of NIST SP 800-63 v2 or equivalent standards (Credential Management, Identity Proofing, Credential Authentication)
  - Kantara Initiative manages the scheme: the assessment rules, approval processes and assessment criteria
  - Kantara Initiative licenses marks of conformity
  - Currently developing a scheme to assess conformity to NIST SP 800-63 v3

© Copyright 2017 Kantara Initiative, Inc.

Information Security Management Systems

- ISO/IEC 27001: *Information technology — Security techniques — Information security management systems — Requirements*
- Requirements for information security management systems
- There are 14 currently-accredited certification bodies in the USA

© Copyright 2017 Kantara Initiative, Inc.

OPEN STANDARDS

© Copyright 2017 Kantara Initiative, Inc.

STANDARDS

[Standards] provide requirements, specifications, guidelines or characteristics that can be used consistently to ensure that […] processes and services are **fit for their purpose**.
— www.iso.org

© Copyright 2017 Kantara Initiative, Inc.

Open Standards

- Cooperation
- Adherence to Principles
- Collective Empowerment
- Availability
- Voluntary Adoption

© Copyright 2017 Kantara Initiative, Inc.

10 Benefits of Open Standards

- Address Market Needs
- Reduce Costs
- Drive Interoperability and Scalability
- Encourage Market Competition
- Leverage Expert Knowledge

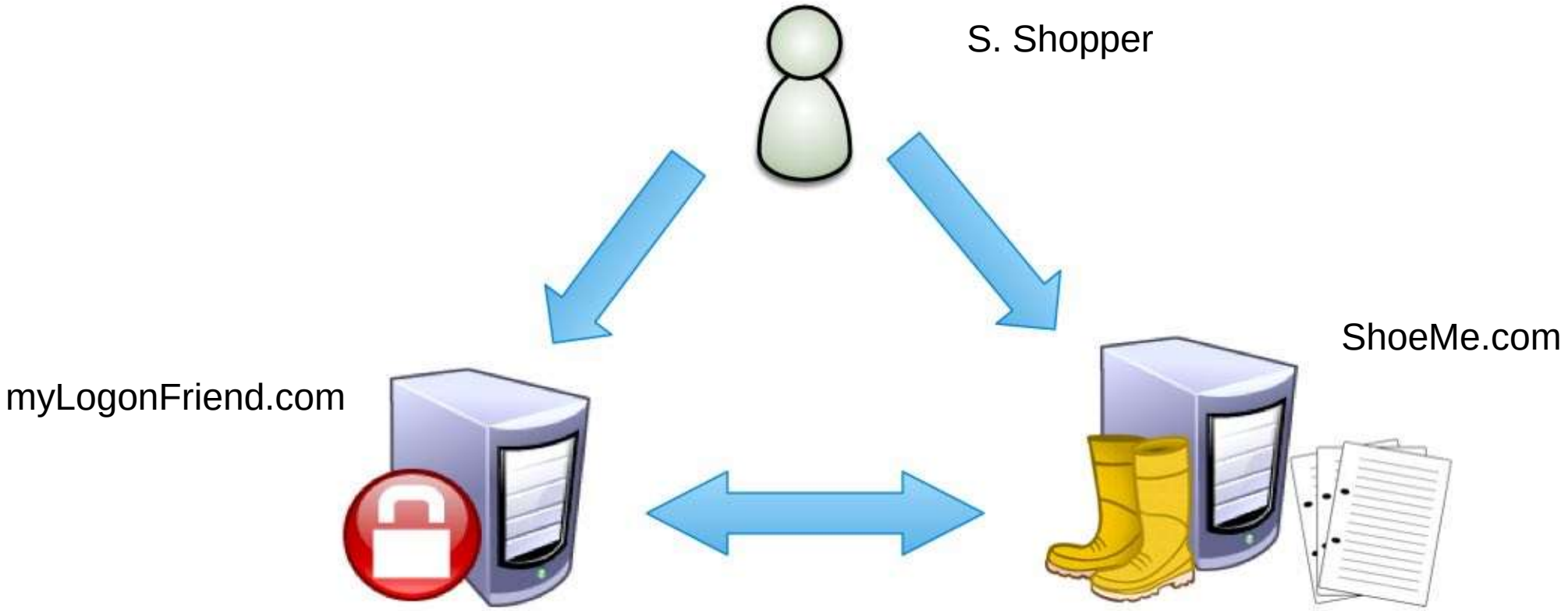
© Copyright 2017 Kantara Initiative, Inc.

A Scenario

SHOEME.COM AND PERSONAL DATA PROTECTION RISKS

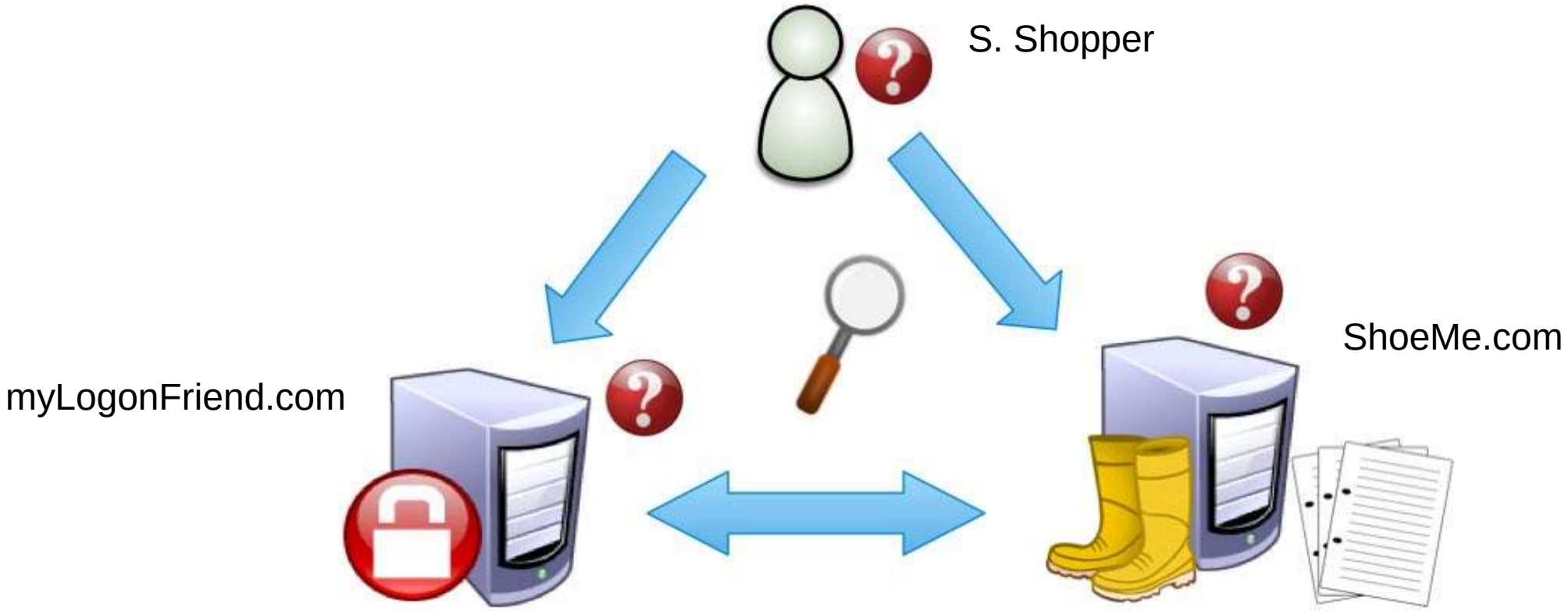
© Copyright 2017 Kantara Initiative, Inc.

Conclusion – ShoeMe.com



© Copyright 2017 Kantara Initiative, Inc.

Conclusion – ShoeMe.com

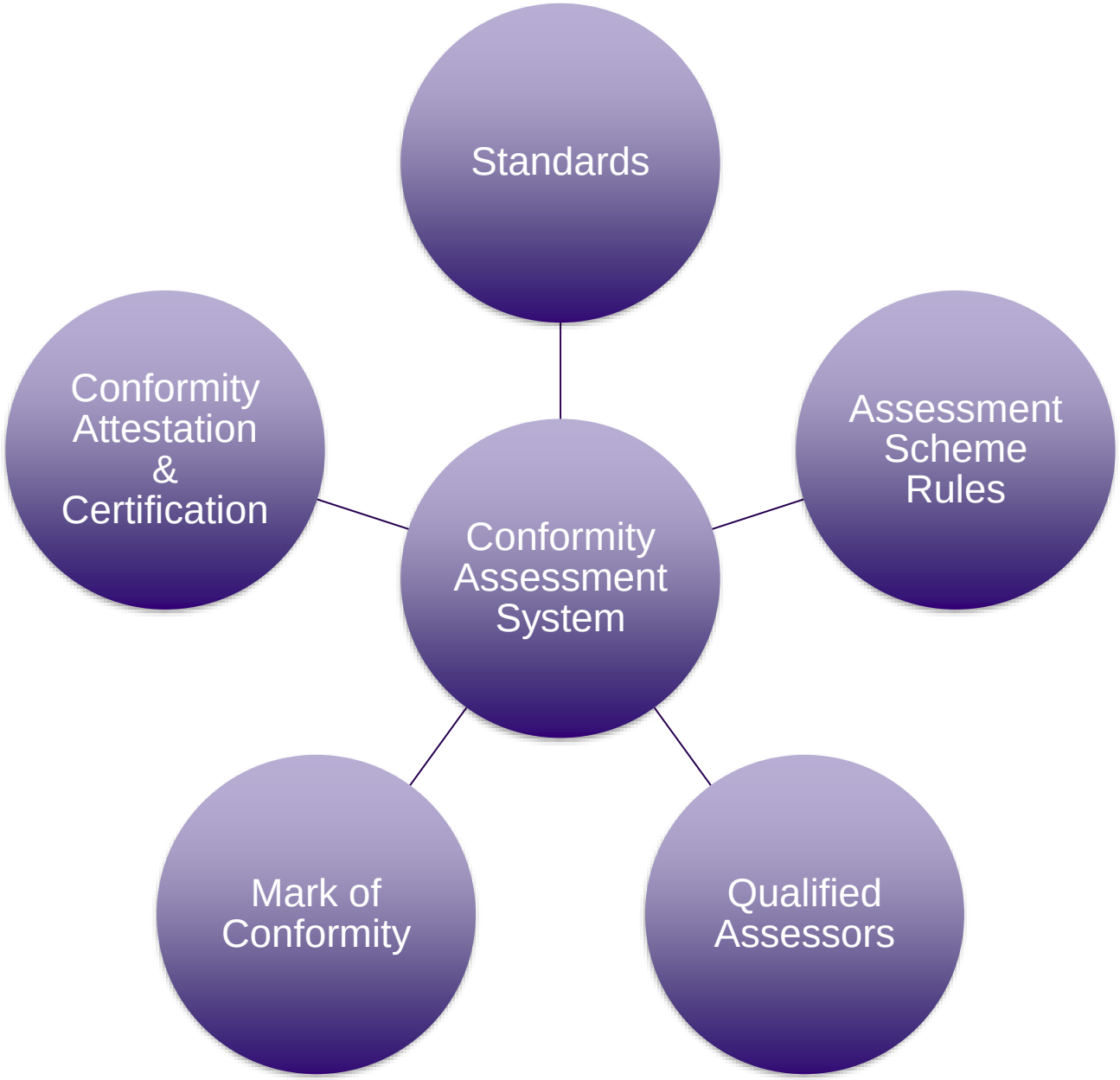


© Copyright 2017 Kantara Initiative, Inc.

Conclusion – ShoeMe.com

© Copyright 2017 Kantara Initiative, Inc.

Conformity Assessment System



© Copyright 2017 Kantara Initiative, Inc.

Join. Innovate. Trust.

The Kantara Initiative is the global consortium improving trustworthy use of identity and personal data through innovation, standardization and good practice

Kantara Leadership Council Chair: AndrewHughes3000@gmail.com
General Inquiries: support@kantarainitiative.org
KantaraInitiative.org

© Copyright 2017 Kantara Initiative, Inc.