E-commerce. business. technology. society. KENNETH C. LAUDON AND CAROL G. TRAVER



video case

- chapter 4 E-commerce Security and Payment Systems
 - case 4 Open ID and Web Security

watch the video at

http://www.youtube.com/watch?v=xcmY8Pk-qEk

- **summary** This video explains the concept and potential operation of OpenID, a method for providing individuals and corporations with a private identity which can be used at all Web sites without re-entering identity information (and sacrificing convenience). *L=4:35.*
 - **Case** OpenID is an open, decentralized standard for user authentication and access control, allowing users to log onto many services with the same digital identity. It is a single sign-on (SSO) method of access control. As such, it replaces the common login process that uses a login-name and a password, by allowing a user to log in once and gain access to the resources of multiple software systems.

An OpenID is in the form of a unique URL, and is authenticated by the user's 'OpenID provider' (that is, the entity hosting their OpenID URL). The OpenID protocol does not rely on a central authority to authenticate a user's identity. Since neither the OpenID protocol nor Web sites requiring identification may mandate a specific type of authentication, non-standard forms of authentication can be used, such as smart cards, biometrics, or ordinary passwords.

As the video mentions, the two benefits of OpenID are convenience and security. As it stands, different sites know individual users in different ways; each site has a unique way of

Annual C

Contraction

identifying its users. And many sites are not prepared to focus on security in a satisfactory way. This is inconvenient for the user and also jeopardizes their personal information when they provide login information for sites that have inadequate privacy protections.

Under OpenID, users would visit sites known as 'relying parties', because these sites rely on identity providers to sign in their users. When a user tries to log in, the relying party asks the identity provider to confirm the user's identity. In turn, the identity provider asks the user to confirm that he trusts this new site. The user doesn't need to fill out any forms or create a new identity and password for that site, and the site doesn't need to worry about protecting the information its users provide.

video case questions

- 1. Explain why OpenID offers users greater convenience and security than the current system.
- 2. What are the possible drawbacks of the OpenID system?
- 3. Would you consider using an identity provider to access content on the Web? Why or why not?
- 4. Why might online businesses be excited about the advent of the OpenID system?

Copyright © 2015 Kenneth C. Laudon and Carol Guercio Traver.

This work is protected by United States copyright laws and is provided solely for the use of instructors in teaching their courses and assessing student learning. Dissemination or sale of any part of this work (including on the World Wide Web) will destroy the integrity of the work and is not permitted. The work and materials from this site should never be made available to students except by instructors using the accompanying text in their classes. All recipients of this work are expected to abide by these restrictions and to honor the intended pedagogical purposes and the needs of other instructors who rely on these materials.