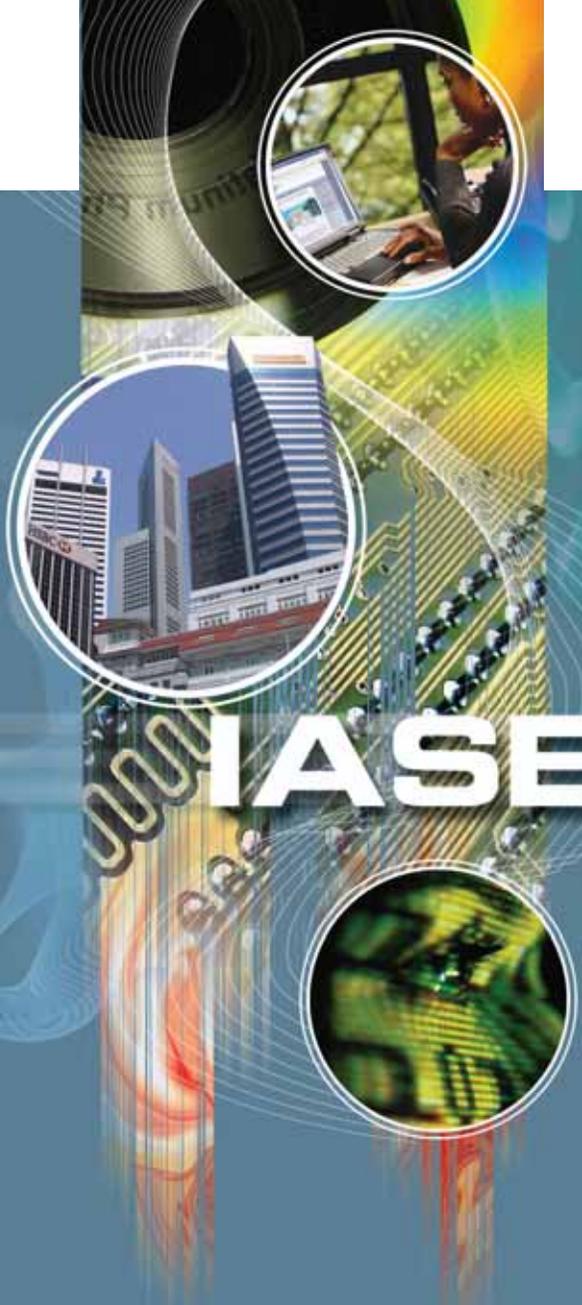# IASE

Founded in 1997 by Professor K.Y. Lam as an advanced security R&D house in Singapore, PrivyLink is geared to meet the strong industrial demands for high-assurance delivery channels in secure electronic transactions and homeland security systems. We have established ourselves as the key innovator of strong security solutions deployed in government departments, financial institutions and corporations. Our products offer adaptive end-to-end security protection for applications and data exchanged over fixed networks and mobile channels. In addition, we have been engaged by reputable organizations to provide consulting services, security review and system design.

IASE

Internet application security environment

PrivyLink was among the first to promote and pioneer end-to-end system security, which has since become an essential system and network design goal in the ICT security industry. Supposedly strong cryptographic systems can be paralyzed by security gaps. We released version one of IASE, short for Internet Application Security Environment, back in 1998/99, this product quickly rose to fame as it plugged the security gaps in our clients' systems. Today, IASE is behind many of the websites of our clients in both the private and public sectors.

For more information, please visit our website at http://www.privylink.com/ or contact us by email: sales@privylink.com.sg

PrivyLink

accountability & end-to-end security

Secure Internet Applications End-to-End

IASE secures Internet applications end-to-end between client browsers and the back-end application servers, hence eliminating any security gap in the web server. Data security can be compromised even when the communication links between the web and application servers are protected, as unprotected data cached in or passing through the web servers is subject to unauthorized access.

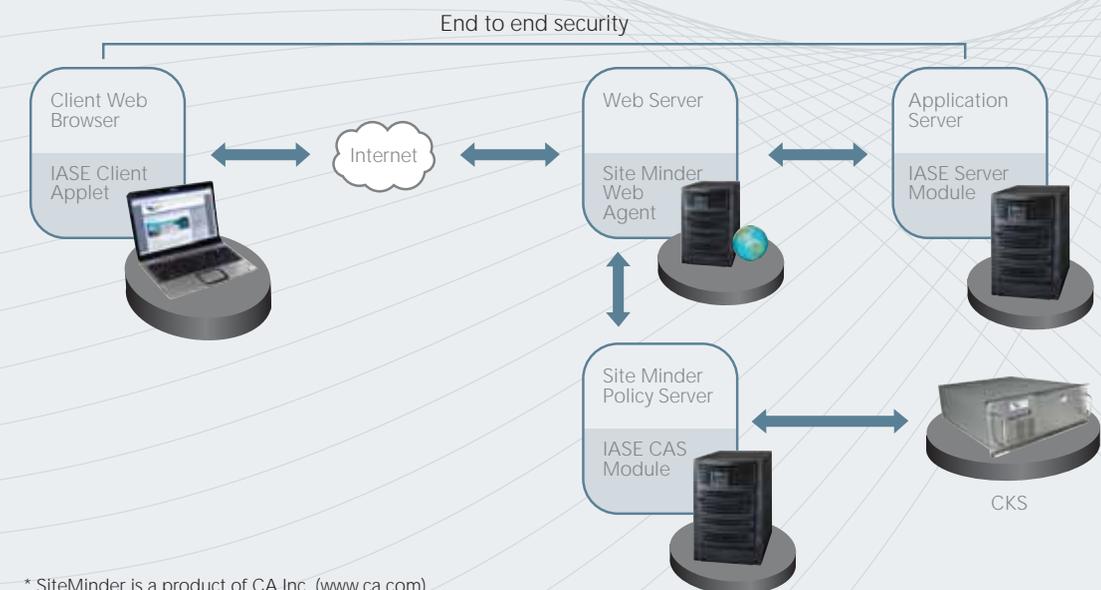IASE can be deployed in a variety of online applications:
- Secure login and authentication
- Internet banking
- Stock trading
- Submission of confidential documents, tenders and tax returns
- Other e-commerce applications
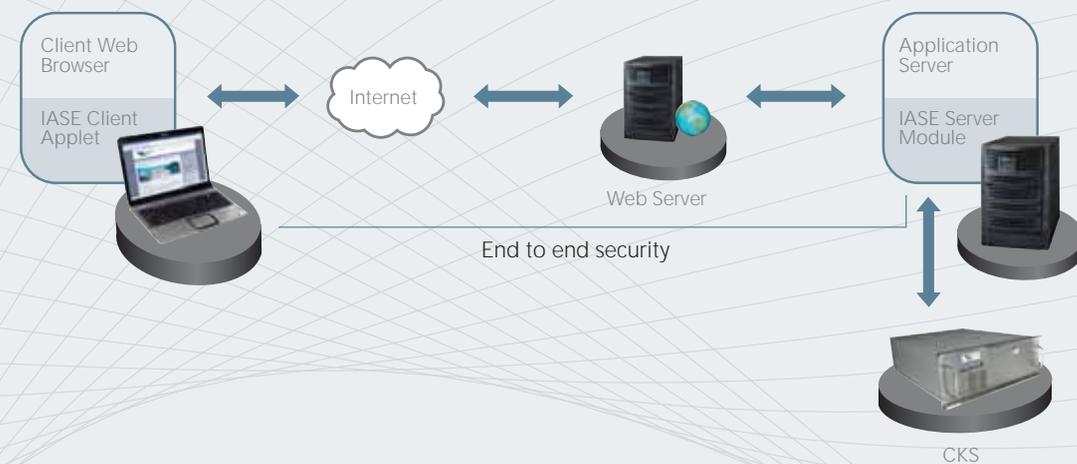
End-to-End Authentication for SiteMinder*

IASE has been deployed to enhance the security level of SiteMinder's SSO authentication application. IASE adds end-to-end security and accountability to SiteMinder, which is a single sign-on and privilege management infrastructure with interface to support advanced third-party authentication schemes.

In addition to the IASE Server Module for the application server, the IASE CAS (customized authentication scheme) Module is required in the SiteMinder Policy Server. The Policy Server directs authentication requests to IASE CAS according to a set of pre-defined security policies. In response, CAS invokes IASE Server Module for processing user credentials and other confidential data in encrypted form, which are sent to the CKS key server for user authentication and other cryptographic operations. CKS is connected to the Policy Server where IASE CAS is loaded.

Diagram (left): End to end security — Client Web Browser / IASE Client Applet → Internet → Web Server → Application Server / IASE Server Module → CKS

Diagram (right): End to end security — Client Web Browser / IASE Client Applet → Internet → Web Server / Site Minder Web Agent → Application Server / IASE Server Module; Site Minder Policy Server / IASE CAS Module → CKS

* SiteMinder is a product of CA Inc. (www.ca.com)

Versatile & Easy to Deploy

The heart of IASE is its Server Module operating from the application server(s) hosted by an application provider. Upon any login or authentication request sent from users' web browsers, the application server may call upon IASE Server Module to return a HTML page embedded with a client applet, which typically carries a cryptographic key and other session dependent data. Next, the user is prompted for his login ID / password and when he submits the data, the client applet generates transparently an encrypted PIN block for subsequent authentication by the IASE Server. Decryption of the PIN block and user authentication is performed within the tamper-resistant environment of PrivyLink's CKS (Cryptographic Key Server), a hardware security module that provides highly secure environment for cryptographic operations and user authentication. Other user-generated confidential data can be encrypted and sent to the IASE Server Module in a similar fashion.

IASE is computationally efficient and bandwidth friendly. The client applets are light weight and they work in any web browsers (PC, PDA, set-top box) that support Java applets. No other special client software is required. Active-X controls may be used for platforms that do not support Java plug-in.

The IASE Server Module requires JRE 1.4.2 or above and it supports MS Windows, Solaris and other popular operating systems. Supported scripting languages include CGI/C, ASP, Java Servlets / JSP and ASP.NET. Dynamic PIN pad may be used to enhance PIN security management.