ImageWare Systems, Inc.

Delivering next-generation biometrics as an interactive and scalable cloud-based service

SUMMARY

Catalyst

ImageWare Systems, Inc. (IWS) is a developer of leading-edge, identity-based, credential management solutions which are driven by biometric technology. Biometric use as a component of secure multi-factor authentication is well established, but has often been limited to highly secure environments. The ImageWare approach of delivering next-generation biometric technology as an interactive and scalable cloud-based service, and providing authentication via the latest range of smart mobile devices, engages IWS with two of the most challenging and at the same time dynamic areas of the technology market.

Key messages

- The IWS CloudID and IWS Identity Service Bus (ISB) products combine to provide an integrated, cloud, and biometric-driven approach to identity and credential management.
- IWS Mobile brings together cloud and mobile technology to offer multi-factor authentication for smart phone users and mobile clients based on the range of biometric models and mainstream authentication techniques supported by IWS.
- The service bus approach enables IWS to provide purpose-built application servers that deliver standards-based business processes for identity and credential management across the full application lifecycle.
- The use of biometrics to provide secure access and authentication is an established market that has operated successfully across business environments where the risks outweigh associated costs, but until recent times, has generally been restricted to these areas.

Ovum view

The growing interest in cloud and mobile device technology opens up new opportunities for the biometric sector, and in particular for organizations, such as IWS, that have invested in the development of cloud-based services to support its extensive range of identity and credential management services.

RECOMMENDATIONS FOR ENTERPRISES

Why put ImageWare Systems Inc. on your radar?

The use of biometric technology within highly secure business environments is well established. Fingerprinting, iris scanning, and facial recognition products are used successfully across highly secure business operations. More recently the market has opened up and become just as effective in support of less demanding operations. The technology is now just as likely to be used by taxi drivers to raise a barrier when leaving an airport car park as it is by technicians entering highly restricted areas, or within the education sector to record that children have eaten their lunch in the school canteen.

The technology and financial barriers that once restricted biometrics to specific highly controlled areas of are coming down. Disruptive business and consumer technologies, including mobile devices and cloud-based services, provide new vehicles for the uptake of biometric solutions. The biometric usage model is being opened up to mainstream use in both secure and everyday business environments, where both single and multi-factor authentication approaches can be applied.

IWS has adapted its enterprise service bus platform and communications facilities to support an integrated approach to the delivery of identity and credential management across all available biometric modes. For example, in the mobile space, IWS supports biometric authentication using voice, fingerprint, and facial recognition. All of which can be combined alongside other authentication and access control facilities including digital certificates, passwords, and PINs. The IWS ISB utilizes cloud services (IWS CloudID) to support the integration of its secure identity and credential management technology into business environments.

HIGHLIGHTS

Background

IWS is a leading provider of biometric identity management solutions. The company has its North American headquarters in San Diego, California and also has offices in Portland, Origon; Washington, D.C.; and Ottawa in Canada. From the time that the company was founded over a decade ago, IWS has focused on developing innovative, patent-protected biometric technology for the identity and credential management marketplace. Its approach of pushing the technology boundaries of identity and credential management continues with The IWS CloudID and IWS ISB platform which enables system integrators and identity services providers to quickly and effectively develop and deploy highly configurable and modular multi-factor biometric-based authentication solutions.

The technology is relevant to public and private sector organizations across all geographies and of all sizes. Vertical markets where IWS has enjoyed particular success include financial services, medical and healthcare organizations, and the retail sector. IWS usage examples include the management of millions of identities for customer groups ranging from the US Veterans Administration through to the Canadian Air Transport Security Authority. The company's credential management software is used to issue identity cards, drivers' licenses, passports, and visas in dozens of countries worldwide, and it is also used by over 100 law enforcement agencies.

Current position

The availability of new generation mobile devices for business and personal use, the development of cloud-based services, and the need to protect users and their access rights has opened up the requirement for both highly secure and simple, more basic identity and credential management solutions. This is the case for both government and private sector organizations and is widening the opportunity for organizations such as IWS that have the proven ability to offer credential management solutions that match the higher and lower level security requirements of most enterprise operations.

IWS CloudID and IWS ISB provide the framework for multi-factor biometric identity and credential management. The methodology incorporates a service oriented architecture (SOA) approach with publish and subscribe mechanisms where application servers expose web services interfaces that integrate with applications and connected clients. As such, the solution and its architecture is open for use in cloud-based service models as well as retaining the ability to support private network, client-server operations.

Over time IWS has adapted its enterprise service bus integration and communications approach to provide a scalable software platform for user-selected biometric products. The approach allows IWS to support purpose-built application servers that deliver interoperable business processes for identity management, credential life-cycle management, and the management of biometric identities.

The patented IWS Biometric Engine is central to the operation. It provides realtime, high-performance, and scalable access to the biometric database. Its security components ensure that only valid users can gain access to controlled areas. The IWS client makes use of web services communications to support interactions between the service bus infrastructure and the clients. Supporting applications and products include:

- The IWS QuickApps facility provides tailored client software to support and interact with the IWS ISB.
- QuickCapture offers multi-biometric enrollment services.
- QuickBadge provides flexible smart-card production and issuance services.
- QuickID is used to provide biometric identity analysis, identification, and identity verification services.

Mobility and the use of cloud-based services are influencing most sectors of the information and identity management markets. New strategies from IWS support the use of these disruptive technologies. Examples include the ability to support identity-based authentication for mobile and online access in the banking sector and for the extended authentication of online transactions. Its approaches are also capable of facilitating anonymous identity authentication for Internet and mobile banking using single and multiple-factor biometrics.

IWS Mobile technology combines patented template-driven messaging for smart phones and mobile clients with multi-factor authentication, including multi-biometric authentication based on the supported range of biometric modes. These include voice and facial recognition which can be combined with other authentication factors such as digital certificates, user-identities, passwords, and PINs.

DATA SHEET

Key facts

Table 1: Data sheet

Product name	IWS CloudID and IWS Identity Service Bus, IWS QuickApps and IWS Mobile	Product classification	Biometric identity management
Version number	V2	Release date	December 2011
Industries covered	Government, financial services and banking, healthcare, telecommunications, and transportation	Geographies covered	All
Relevant company sizes	Small, medium, and large	Licensing options	Perpetual and term options: per seat clients, per server, and per biometric enrollment. SaaS: as above, or optional service subscription models based on levels of use
URL	www.iwsinc.com	Route(s) to market	Direct sales and via VAR channels
Company headquarters	10815 Rancho Bernardo Rd Suite 310 San Diego, CA 92127 USA		

Source: Ovum

APPENDIX

"On the Radar"

"On the Radar" is part of Ovum's series of research notes that highlights up-and-coming vendors that bring innovative ideas, products, or business models to their markets. Although "On the Radar" vendors are not always ready for prime time, they bear watching for their impact on markets and could be suitable for certain enterprise and public sector IT organizations.

Further reading

- Security challenges in the authentication sector, analyst insight report, IT017-004180, August 2013
- Cloud: Transforming the IAM industry, analyst insight report, IT017-004036, July 2013

Author

Andrew Kellett, Principal Analyst, Infrastructure and Security

Andrew.kellett@ovum.com

Disclaimer

The facts of this report are believed to be correct at the time of publication but cannot be guaranteed. Please note that the findings, conclusions, and recommendations that Ovum delivers will be based on information gathered in good faith from both primary and secondary sources, whose accuracy we are not always in a position to guarantee. As such Ovum can accept no liability whatever for actions taken based on any information that may subsequently prove to be incorrect.