

Technology Audit

Security

ActivIdentity Smart Employee ID

Written by: Alan Rodger

Date: January 2007

Abstract

Smart Employee ID, from ActivIdentity, is an enterprise-strength, end-to-end solution for credential management and authentication that provides capabilities over a range of authentication types (passwords, smartcards, PKI, and SSO), and valuably facilitates use of these in combination where appropriate. Many organisations find that compliance and risk pressures are driving them towards adopting stronger authentication of user identity, and smartcards are seen as a versatile option that can incorporate the advantages of multiple authentication technologies. As smartcards are also used in many physical access systems for premises, there are significant efficiency and process benefits in considering solutions to unify the management of access to 'physical' buildings and facilities with that to IT ('logical') resources, and this is an area in which the ActivIdentity solution has market-leading strengths. For organisations seeking to deploy a single, secure employee ID badge for access to logical and physical resources, ActivIdentity provides a Smart Employee ID solution that reduces administration costs, increases security, and improves user convenience. The smartcard functions as a photo ID and a proximity badge for facility access, as well as an IT security device for strong authentication to information systems, for data security, and for digital signature.

Butler Group believes that ActivIdentity could consider strengthening the solution further by incorporating SSO for users external to the enterprise – however, it does offer seamless integration with the market-leading third-party solutions, and can extend these with its strong authentication capabilities. Indeed, ActivIdentity is one of the leading exponents in its particular area of the overall Identity and Access Management (I&AM) marketplace, and offers customers increased value via its facilitation of modular adoption, and by providing excellent integration with other providers' complementary I&AM products that cover areas such as provisioning.

KEY FINDINGS

Key: ✓ Product Strength ✗ Product Weakness ⓘ Point of Information

✓	Provides integrated solutions across a wide range of credential-related needs.	✓	Strong capabilities for integration with third-party identity management features, for example provisioning.
✓	Integrates logical and physical (badge-based) access, incorporating efficiency gains.	✓	Flexible approach to authentication technology adoption, providing an upgrade path to stronger security.
✗	Does not offer SSO for users that are external to the enterprise (e.g. Web-based customers).		

LOOK AHEAD

ActivIdentity is working with several providers towards enabling delivery as a managed service, probably with a yearly subscription model. Managed services for smartcard lifecycle management and authentication will be offered to both government and enterprise organisations.

► FUNCTIONALITY

Product Analysis

The ActivIdentity Smart Employee ID solution is an integrated and modular suite of products that enables organisations to readily address a range of business security credential needs, using: multi-function smartcards that can carry both photo and electronic credentials; USB tokens that provide the same functionality as smartcards without requiring deployment of readers; passwords; tokens that generate One-Time Passwords (OTPs), and so enable strong authentication; and Public Key Infrastructure (PKI) credentials. These can address a wide range of requirements including:

- Secure workstation and network access, including:
 - Login with strong authentication, such as that based on PKI to desktops, whether they are on-line or off-line.
 - Pre-boot login.
 - Network access to Local Area Network (LAN), or Wireless LAN (WLAN).
- Secure remote access, enabling full authentication, authorisation, and administration of employees who need to access corporate IT resources remotely using Virtual Private Networks (VPNs), Web, WLAN, or terminal services.
- Single Sign On (SSO) and Password Reset, combining strong security based on two-factor authentication with potential cost savings from a self-service approach that avoids help desk-related delays.
- Data security, including Digital Signature, which can be used to add file encryption, document security, and signed or encrypted e-mails to the corporate protection arsenal.
- Smartcard lifecycle management: the solution can manage the cards themselves throughout their entire lifecycle, as well as the distribution and management of data, applets, digital credentials (including PKI certificates), and other information relevant to the cards.
- Physical access integration, as the solution can tightly integrate with leading physical access control systems that provide secure access to buildings and other facilities, thereby enhancing security and efficiency by enabling this type of facility to be managed along with access to IT resources.

Importantly, the solution takes account of the need to leverage organisations' existing IT assets and infrastructures, and facilitates integration with enterprise directories, physical access systems, and PKI services to streamline the issuance and administration of digital identities. Within the wider framework of I&AM and security, it also provides integration with a broad range of enterprise provisioning systems (including those from IBM, Sun Microsystems, Novell, and CA), and with physical access control systems from market-leading partners (including AMAG, Hirsch, Honeywell, and Lenel), these latter integrations permitting the smartcard to be issued and managed directly from the physical access badging application, a feature which ActivIdentity states is unique to this solution. As well as these out-of-the-box capabilities, the solution provides a software development kit which enables customised integration with any Certificate Authority (using the Credential Provider Interface API), further provisioning systems, and external data sources from which data to be stored on smartcards might need to be imported (using the workflow plug-in interfaces).

Butler Group believes it a major strength of the solution that such a range of functionality is included, while being very helpfully adaptable to customisation requirements, and marketed such as to allow adoption as needed to suit individual organisations' security and business requirements. Competing security solutions generally address only a subset of the range of business needs that this solution caters for: ActivIdentity's Smart Employee ID solution delivers an all-in-one employee ID solution consisting of physical access and the full range of logical access capabilities including secure desktop, network, and remote access, SSO, and credential and device management.

Product Operation

The following products within the solution provide the core of card management services, and card usage enablement services:

- **ActivID™ Card Management System (CMS)**, which manages the issuance and administration required for smartcard deployments throughout the card lifecycle, up to and including revocation, incorporating both the cards themselves and the data, applets, digital credentials, and other information that is stored on the cards. It provides integration with third-party directory and certificate authority services, as well as building access, and provisioning, systems to enable greater efficiency to be driven into operational management of these processes across organisations' end-to-end requirements.
- **ActivClient™**, which provides the PC interface that allows the solution to deliver multi-factor, strong authentication to a variety of services on client machines. Consisting of PC-based software, and a smartcard reader/writer (where smartcards are in use), it offers the necessary interfaces so that smartcards and USB tokens can deliver PKI and OTP services, thereby enhancing PC and network security. It also enables the use of smartcards for secure workstation and network access, secure remote access, and can provide 'PC locking' when the card is removed. Additionally, it allows users' PKI credentials stored on the smartcard to be used for applications such as secure e-mail, digital signatures, and secure Web access.

The solution also includes the following products, offering optional added functionality:

- **ActivIdentity 4TRESS™ AAA Server**, an enterprise-strength authentication server offering full Authentication, Authorisation, and Accounting services, and full integration with existing remote access network infrastructure (e.g. dial-up, VPN, Web access, and other facilities). These services protect enterprise assets by validating and tracking user identity across a network, regardless of entry point. The server is RADIUS, TACACS+, and 802.1X compliant and enables deployment of two-factor authentication devices including OTP tokens, soft tokens, USB tokens, and smartcards by providing validation services of the OTPs generated by these devices.
- **ActivIdentity SecureLogin® SSO**, which provides centralised sign-on and access rights assignment for all end-user accesses to applications and IT assets. It supports automatic login to a wide range of applications (Windows-, Web-, and Java-based, as well as on terminal emulators), and it leverages the directory's definitions of enterprise users and assets, and the directory's distribution mechanism to manage up-to-date access rights according to centralised policy definitions. As well as sign-on, it can be used to manage events such as expiry on the user's behalf throughout the password lifecycle. In addition to the benefits of reduced helpdesk support costs for password resets, if combined with smartcard deployment SecureLogin SSO provides extra security, and guarantees that the access to the user credentials is protected using the smartcard-based network authentication. Due to the requirement to access SecureLogin SSO via a client component, and the need for users accessing the product to be defined in the corporate directory, it cannot be used to enrol users external to the enterprise (e.g. first-time e-commerce customers).

Typical enterprise use of various credential types is shown in the context of the solution, in Figure 1.

During the smartcard issuance phase, CMS connects to the enterprise directory and Certificate Authority to generate credentials and load them onto the user's smartcard. Optionally, CMS can also connect to the 4TRESS™ AAA Server to generate credentials necessary to generate OTPs, and load those on to the smartcard. The user's smartcard-based credentials are presented to applications via the smartcard reader, which may be internal (e.g. for laptops using a PCMCIA slot) or attached externally via a USB interface. PKI credentials can be used for a variety of operations such as Windows Login, Secure Web access, e-mail signing, and encryption. ActivClient includes Microsoft CAPI and PKCS#11 libraries to provide compatibility with a wide range of PKI-enabled applications.

For remote access applications that are not PKI-enabled (e.g. IPSEC- or SSL-based VPN), ActivClient can generate an OTP from the credentials on the smartcard, and submit it to the remote access application, which will forward the authentication request to the 4TRESS™ AAA Server for authentication. If alternative OTP-generating hardware tokens are used, 4TRESS AAA Server can validate these without ActivClient being involved.

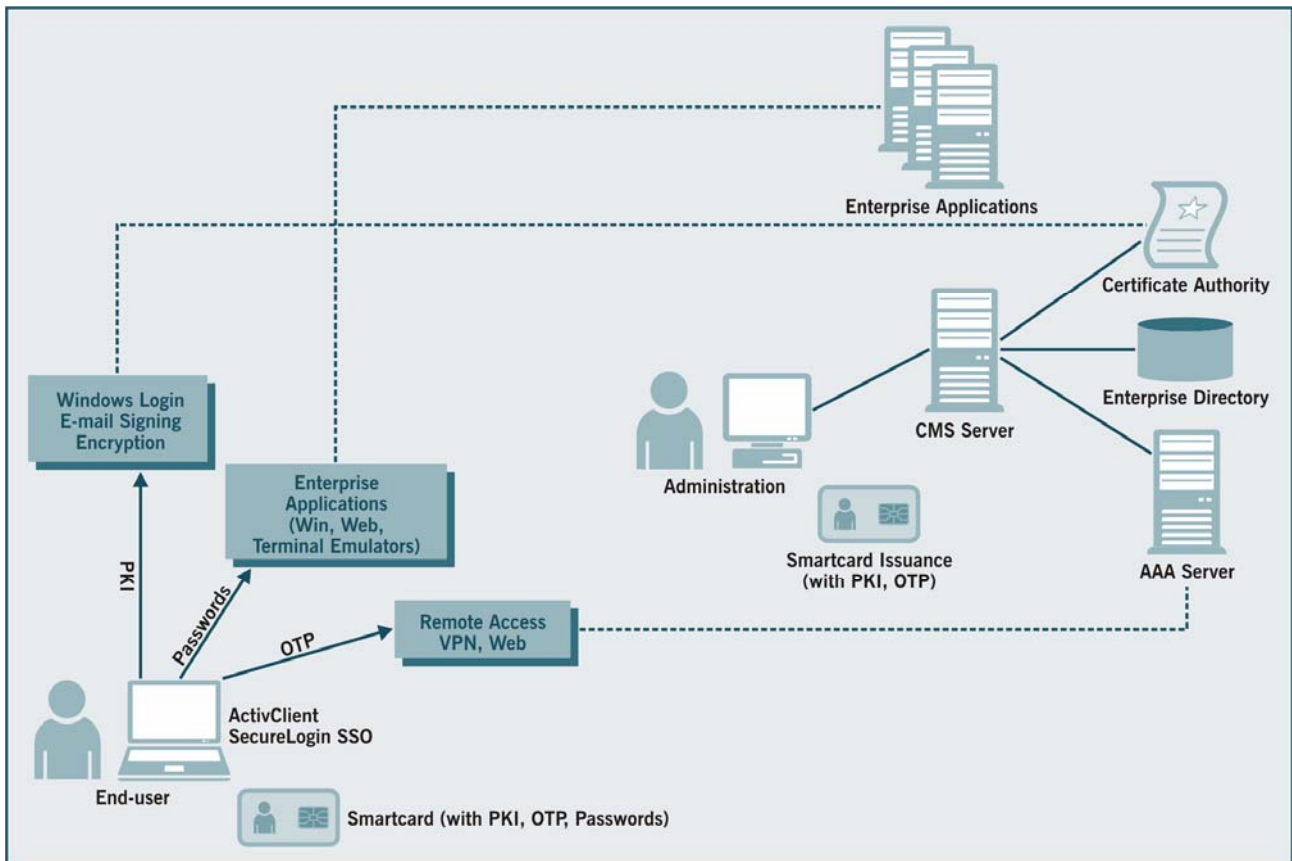


Figure 1: Typical Uses of Smart Employee ID

Product Emphasis

This solution offers a wealth of options to incorporate increased efficiency into measures to enhance security protection via strong, reliable authentication, and the flexibility to choose an adoption path that suits the individual organisation. In offering extensive integration features to data sources and systems that constitute legacy identity authentication, and thereby allowing the value of existing investments to be preserved, it also helps to address a factor that is a difficulty for many organisations that wish to upgrade their identity authentication capabilities. Its position of leadership in offering well-managed integration of logical and physical access will be a major strength as large organisations recognising the value of smartcards increasingly adopt this approach.

While Butler Group feels the range of solution features would be completed by Web-based SSO for customers unknown to the organisation, it does integrate seamlessly with (and can add value to) the leading third-party solutions, and already offers access to an extremely synergistic range of authentication technology options that will provide a wide enough choice for almost any organisation’s authentication requirements for internal users.

► DEPLOYMENT

The resources required to implement the solution are dependent on which capabilities are deployed, and ActivIdentity estimates that deployment of CMS without integration with a physical access system requires a programme manager and a Consultant from the vendor’s professional services team, with a project manager, security architect, two or three IT administrators, and one or two help desk employees from the customer organisation. Additional integration with a physical access system typically requires two staff with physical access responsibility (e.g. facilities or security management). Some engagements have been completed in less than four months, but a typical engagement of all end-to-end functionality takes six to 12 months from best practices consulting through to deployment.

The solution very strongly supports a modular approach to deployment or adoption. For example, ActivClient can operate in standalone mode, providing smartcard PKI capability and enabling a range of applications to leverage PKI authentication, although this approach would lack central configuration and management capability. The most common enterprise deployment is based on the combination of CMS and ActivClient. The solution is designed to leverage existing enterprise resources (e.g. corporate directory, and certificate server) as much as possible, and also industry standards such as the SQL database. When integration with a physical access system is undertaken, organisations can use existing badge issuance processes if necessary, to minimise re-training. After smartcards are issued, many common maintenance operations (e.g. unlocking the card after multiple wrong PIN entries, or updating applications on the card) can be performed directly by end-users with self-service facilities through the “My Digital ID Card” portal within ActivID™ CMS.

Standard product certification training is available for each of the solution areas, and ActivIdentity's professional services staff also provides product level knowledge transfer as part of deployment services. In-depth technical training for administrators is also available, and training programmes can be undertaken at ActivIdentity offices, or at customer sites. Some Web-based training is available, although this is mostly appropriate for upgrades.

The solution is supported primarily on the Microsoft Windows platform, both for the client and server products. ActivIdentity also provides support for UNIX environments; ActivID CMS is available on Solaris; and ActivClient is also available on Solaris and Linux. ActivID CMS requires a relational database, for which Microsoft SQL Server or Oracle's database is supported, and ActivID CMS also leverages a corporate directory as the user repository (for which Active Directory, or any LDAP directory is appropriate). ActivIdentity 4TRESS AAA Server can be deployed with a built-in database, or can leverage a Microsoft SQL Server or Oracle database for increased scalability and fault tolerance, and it also leverages the corporate directory as the user repository. ActivClient and SecureLogin SSO do not have any database or application server requirement. SecureLogin SSO leverages a corporate directory as the user repository and SSO credential store.

ActivClient and SecureLogin are tightly integrated, creating a highly secure SSO environment, in that for example the user's SSO application credentials are stored and protected on a smartcard, and the SSO data stores in the directory are protected with PKI-based encryption that is enabled by the smartcard. It is also designed to integrate seamlessly on the user desktop to minimise process changes, and indeed to simplify the user experience and therefore increase productivity – for example:

- In a Windows PKI login, the user enters a Smart Card PIN instead of a Password.
- In a VPN login based on OTP, the user enters a Smart Card PIN, prompting the username and OTP to be entered automatically.
- In a login to a SSO-enabled application, SecureLogin SSO automatically enters the application-specific username and password on behalf of the user, who therefore does not have to take any action.

► PRODUCT STRATEGY

ActivIdentity provides organisations with the ability to issue users with one strong identity, and to force them to authenticate this through one, or a combination of, strong forms of identification. With SSO also forming part of the solution set available, security is increased because account management is removed from user control, while each back-end system is protected by the strict enforcement of password policy. If stronger authentication is a prerequisite for access to certain applications, multi-factor authentication can be mandated when needed. ActivIdentity also provides opportunities for enterprises to leverage their investment in either physical or logical access systems to gain integration benefits, and to integrate provisioning of SSO credentials onto employees' access cards.

The solution would deliver benefits to organisations in many vertical sectors, and is targeted in general at large global organisations such as the Fortune 1000, and Forbes Global 2000. Organisations in the government, healthcare, and financial services sectors are also seen as key targets, due to particular requirements arising from regulatory or legislative compliance e.g. Homeland Security Presidential Directive #12 (HSPD12), and the Health Insurance Portability and Accountability Act (HIPAA), in the US. ActivIdentity may also benefit in business terms from the various national identity programmes in progress or under consideration.

Target organisations with 10,000 or more employees are subject to direct sales engagements as well as with system integrators, whereas organisations smaller than this are engaged by ActivIdentity’s partner network of accredited distributors and resellers. As well as these, the solution is sold by a number of well-known Global Alliance partners (HP, IBM, Novell, Northrop Grumman, Sun Microsystems, and VeriSign) and Global Service Partners (EDS, IBM, BT, Logica CMG, BearingPoint, IdentiPhi/Dell, Lenovo, and Oracle). SecureLogin is a key part of Novell’s I&AM solution set, via an OEM agreement, and ActivIdentity solutions provide out-of-the-box integrations with I&AM solutions from IBM Tivoli, Sun Microsystems, and Novell. The company also has a long list of technology partners, as follows:

<ul style="list-style-type: none"> • AMAG® • Adobe • CA • Checkpoint • Cisco • Citrix • Cybertrust • Entrust • Gemalto • GE® Security • Giesecke & Devrient (G&D) • HID 	<ul style="list-style-type: none"> • Hirsch Electronics • Honeywell • IBM • Lenel Systems International • Microsoft • nCipher • Novell • Oberthur Card Systems • Omnikey • Oracle • PointSec • SafeBoot 	<ul style="list-style-type: none"> • Safenet • SCM Microsystems • Sun • Tyco / Software House • VeriSign • WinMagic
		<p>Government Sector Only</p> <ul style="list-style-type: none"> • Daon • Intellisoft • IWS™ • Viisage

The solution is priced per user, and uses a perpetual licence model. The price for the basic solution (ActivID CMS and ActivClient) is US\$52 per user for 2,500 users. The full Smart Employee ID solution, including Strong Authentication for Remote Access and SSO modules is priced at US\$113 per user for 2,500 users. In both cases, significant discounting is available at higher volumes. The cost of maintenance and support is 20% of license cost for standard support, or 25% for premium support. Maintenance grants customers access to ActivIdentity software updates and upgrades, and includes hot fixes to address site-specific product issues, as well as periodic patch releases that contain one or more defect repairs. Software upgrades include access to new major releases of ActivIdentity products, containing significant feature enhancements.

Professional services is typically between 10% and 25% of the overall cost, but this is dependent on the size and complexity of the deployment. Activities for which professional services are required commonly include programme management, best practice assessment, planning and analysis, design and build, custom card profile analysis, pilot deployment and training, production deployment and training, and roll-out services. The company states that a solution for 10,000 users in which the full range of capabilities is deployed, and professional services used to the usual extent, would normally achieve benefits within two years that cover the implementation costs (including those of business users’ time commitment), and deliver significant savings continuously thereafter.

Future product developments are planned using feedback from customers and delivered as updates on an annual basis. ActivIdentity is working with providers towards enabling delivery as a managed service, probably with a yearly subscription model.

► COMPANY PROFILE

ActivIdentity was formed in 2005, when ActivCard took a new name following its acquisition of Protocom earlier that year. Both were established vendors in the I&AM market, with highly complementary portfolios: ActivCard’s main focus within the market was authentication, remote access management, and smartcard management systems; Protocom’s, enterprise SSO. The company is headquartered in Fremont, California, and has development centers in the United States, Australia, and France, and sales and service centers in more than ten countries.

It has 310 employees, of whom 116 are based in the EMEA region, 124 in North America, and 70 in Asia Pacific. Around 40% of the workforce is involved with Research and Development (R&D), 29% in sales and marketing activities, 16% in services or customer support, and the remainder have administrative or other operational roles.

Its shares are traded publicly on the NASDAQ (ACTI), on which exchange ActivCard was listed in 2001. Its financial results in recently completed financial years, showing consolidated figures of the merged companies, were as follows:

Year (see notes below)	2006 ¹	2005 ¹	2004 ²
Revenue (US\$ million):	53.4	42.2	33.6
% change	26.5%	25.6%	n/a
Gross Margin:	62.9%	55%	57.5%

Notes:

1 – Revenues reported are for the 12-month periods ended 30 September.

2 – Revenues reported are for the four quarters ended 30 September 2004.

The company has a wealth of products whose technologies combine as solutions for SSO, strong authentication, secure information and transactions, as well as device and credential management. It offers packaged solutions that tailor its technology to the enterprise, government, financial services, and healthcare markets. The convergence of the market areas addressed by ActivCard and Procom, given the need for strong authentication security to protect the added value bestowed by SSO, provides the motivation for the acquisition, and an opportunity for ActivIdentity. In particular, a presidential directive (HSPD12) in the USA decrees that all new employees must have a common access card by October 2006, creating a market for solutions in which ActivIdentity has had significant success: it won a contract to provide 10 million smartcards for the US Department of Defense, covering implementations in all three major military services. BT, ABN Amro, Nissan Europe, Renault, Saudi Aramco, Deloitte, Gallaher Group PLC, Sun Microsystems, AREVA, Crédit Agricole, BNP Paribas, and the Singapore Defence Department, are also major customers. Sun Microsystems is deploying the solution to employees and contractors worldwide totalling approximately 40,000 users. Overall, ActivIdentity has over 4,000 organisations as customers, with over 20 million users of its solutions.

► SUMMARY

The complementary logic of the deal that brought together the two companies to form ActivIdentity is readily apparent in its Smart Employee ID solution. Organisations implementing SSO have been increasingly wary of users' entire access rights being protected only by a single password – the range of capabilities that ActivIdentity offers enables customers to enhance the protection around SSO with secondary strong authentication technologies using PKI, but also to benefit in many additional ways from its strong protection technologies. With the smartcard as the user's portable protection enforcement mechanism, capabilities such as file encryption, document security, and signed or encrypted e-mails can be made readily available, providing much stronger security across applications used every day in business.

As well as providing the means to manage organisations' smartcard estates throughout the lifecycle from issue to revocation, including updating and managing the on-board data throughout that lifespan, the solution also enables management of access to physical resources (when the card is used as an access badge) via leading providers' systems to be unified with the capabilities to control access to IT resources, thereby enabling efficiency savings and more effective processes that can aid compliance. Butler Group believes that organisations in many industries should consider the various ways in which they could adopt better authentication and protection solutions, and reap some of the manifold potential benefits of holistic and up-to-date security management that are available from this solution.

Contact Details

ActivIdentity Europe

24-28 Avenue du Général de Gaulle
92156 Suresnes, Cedex
France

Tel: +33 (0) 1.42.04.84.00

Fax: +33 (0) 1.42.04.84.84

www.ActivIdentity.com

Corporate Headquarters

6623 Dumbarton Circle
Fremont, California 94555
USA

Tel: +1.510.574.0100

Fax: +1.510.574.0101



Headquarters:

Europa House,
184 Ferensway,
Hull, East Yorkshire,
HU1 3UT, UK

Tel: +44 (0)1482 586149

Fax: +44 (0)1482 323577

Australian Sales Office:

Butler Direct Pty Ltd., Level 21,
Tower 2, Darling Park,
201 Sussex Street,
Sydney NSW 2000, Australia

Tel: + 61 (0)2 9955 6249

Fax: + 61 (0)2 9006 1282

End User Sales Office (USA):

Butler Group,
245 Fifth Avenue, 4th Floor,
New York, NY 10016,
USA

Tel: +1 212 652 5302

Fax: +1 212 686 2626

Important Notice

This report contains data and information up-to-date and correct to the best of our knowledge at the time of preparation. The data and information comes from a variety of sources outside our direct control, therefore Butler Direct Limited cannot give any guarantees relating to the content of this report. Ultimate responsibility for all interpretations of, and use of, data, information and commentary in this report remains with you. Butler Direct Limited will not be liable for any interpretations or decisions made by you.

For more information on Butler Group's Subscription Services please contact one of the local offices above.