SOLUTION BRIEF
CA IDENTITY SUITE — IDENTITY MANAGEMENT

Simplify Identity Management with the CA Identity Suite

ca technologies

Section 1: Challenge

Identity Management Challenges

Managing and governing "who has access to what" remains the foundation of any effective security architecture. However, there are several other identity-related challenges that must be met in order to ensure high security, efficiency and usability:

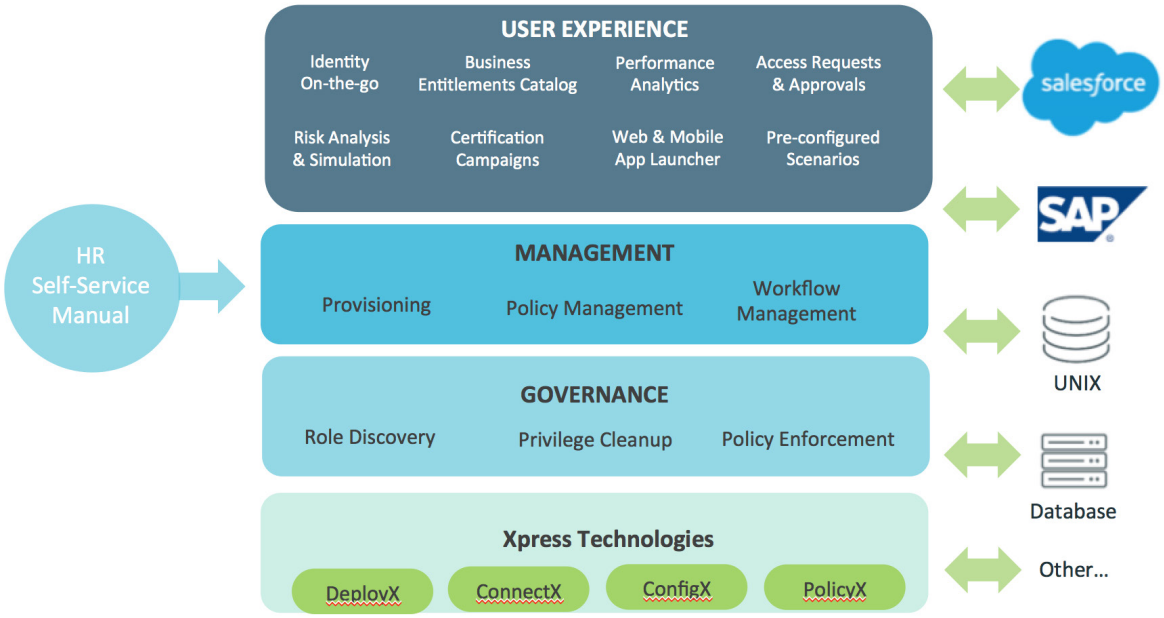
- **Poor user experience**—Identity services are often plagued with inconvenient user interfaces that focus on the IT savvy user rather than the business user. This reduces user satisfaction and hinders more widespread adoption across the enterprise.
- **Ineffective role foundations**—It is common for organizations to have far too many roles defined, poor assignment of privileges to roles or over-accumulation of roles by users. A poor role model creates administrative inefficiencies and increases the risk of improper access.
- **Risks from users with excessive privileges**—Users accumulate privileges over time and frequently end up with access to systems which they no longer need or use, creating the potential for inadvertent or malicious use of privileges.
- **Difficult deployment**—Identity management solutions often require extensive effort just to get some basic use cases developed and deployed.
- **Difficult application connectivity**—Many organizations need to provision users to a wide range of applications and systems, and some of these are often not supported by most provisioning solutions. As a result, custom connectors must be developed, leading to increased development and ongoing maintenance costs.

The basic processes of managing identities and entitlements is well-understood, and solutions exist that do a reasonable job at it. But these solutions often do not meet the needs of today's hybrid, complex environments supporting huge numbers of often mobile users. These users need access to identity services that provide a business-oriented experience that enables, rather than hinders, them to get their job done.

Section 2: Opportunity

CA Identity Suite—Key Identity Management Capabilities

The CA Identity Suite is an integrated suite of identity management and governance capabilities that combine robust functionality with an intuitive, convenient and business-oriented experience. By improving business user productivity and satisfaction, the CA Identity Suite user experience is designed to dramatically increase the identity and access management solution value proposition for large enterprises while removing a significant administrative burden from the IT organization. The components of CA Identity Suite are represented by the following graphic:



CA Identity Suite also delivers core enterprise-grade identity management and governance capabilities, including broad provisioning support for on-premises and cloud apps and consumer-grade scale. The identity management capabilities of CA Identity Suite are contained within CA Identity Manager. The key capabilities of this component include:

User experience for the business user

Often, the user experience for basic identity management functions, like provisioning, is oriented towards the IT savvy user, with names for resources and access rights that are often cryptic and IT-centric. The combination of CA Identity Manager and the CA Identity Portal enables business users to easily leverage identity services because of the simple, intuitive, business-oriented user experience that it provides. No longer must basic identity services be performed only by IT or IT knowledgeable people. For example, a business entitlements catalogue maps cryptic resource names to business terms that are intuitive and familiar to all users. Because these identity services are now so easy to use, user satisfaction and the level of use of identity services across the enterprise both generally increase.

User Self-Service

Providing a convenient, business-oriented experience is necessary, but not sufficient, for improved user satisfaction and productivity. It is also important to let users manage their own information (subject to security policies) so that they don't have to tax the IT help desk resources.

The CA Identity Suite includes broad capabilities to enable secure self-service for users. These capabilities include:

- **Identity dashboard** provides convenient, centralized access to "all things identity" for each user. Information such as user profile, current access rights, risk level and user activity are all available in one place, eliminating the need to engage IT either to obtain or change user identity information. Administrators still retain granular control over what attributes can be changed by each user.
- **Self-registration** enables users to register for Web applications through a publicly available Web page. The user interface can be easily configured to request the specific information required by the organization depending on the type of user. This capability is frequently used for the purpose of managing external users of consumer-based applications.
- **Forgotten passwords and password resets** enable users to identify themselves via alternative means of authentication such as a series of custom questions instead of calling the help desk to reset a forgotten password.
- **Access requests** allow users to request additional access using a simple shopping cart model. Access to resources is done through a business entitlements catalog, which maps often confusing IT-centric resource names into business terms that everybody can understand. The process of requesting access is therefore much simpler than when IT-centric names are used.

Intuitive, business-oriented user experience drives improved user satisfaction and engagement

User Provisioning

Provisioning involves automating the process of adding, modifying and deleting users and their attributes. This includes managing users' profile attributes, including their role memberships and their associated access rights. CA Identity Manager supports these operations and goes beyond the traditional boundaries of organizations to automate these processes across the extended enterprise.

- **Wizard-based on-boarding of new users** (including self-registration) includes users such as employees, business partners and contractors. User on-boarding is simple and intuitive, due to the business-oriented user experience provided by the CA Identity Suite. In addition, transactions can be scheduled for future execution based on date/time criteria. This is helpful especially for contractors who have a defined start and end date.
- **Customizable workflows** support the unique way each organization approves and schedules these activities. This workflow is highly flexible and capable of supporting varying business requirements through template definition, escalation, parallel approvals, serial approvals and multi-step approvals.
- **Broad set of connectors to target systems** CA Identity Manager provide a broad set of pre-built connectors that provide provisioning integration with many popular Web, client-server and mainframe applications, including major computing platforms, enterprise applications, databases, collaboration environments and industry-standard interfaces. These connectors provide deep functionality, to help reduce the need for any custom coding to support unique local requirements.
- **Connector Xpress** is a wizard-driven utility that enables you to generate custom connectors via a graphical user interface without coding. This capability greatly reduces the level of technical expertise required for creating connectors and enables the creation of custom connectors within hours rather than days or weeks.

Simplified, Streamlined Deployment

CA Identity Manager can be deployed very easily through the use of two capabilities.

Deployment Xpress consists of a collection of preconfigured user scenarios for common user cases that most organizations would typically require, such as user onboarding, password reset, access certifications, partner onboarding and the like. Each scenario consists of all elements needed for an easy deployment, such as template user interfaces, workflows and policy definitions. The manager simply picks the scenarios you need, puts them in the shopping cart and then submits them. At that point, all of these key elements are automatically loaded into Identity Suite and deployed. These scenarios speed the deployment process and can significantly reduce the time-to-value for deployment of typical identity services.

In addition, a virtual appliance deployment delivers a pre-installed, preconfigured virtual machine image, ready to run in production configurations under common virtualization platforms. The Virtual Appliance embeds a hardened operating system, application server and the CA Identity Suite software. CA Identity Manager can be installed and configured literally in minutes rather than hours or days as with other solutions.

Fine-Grained Entitlement Management

CA Identity Manager can manage entitlements at a range of depths, from coarse- to fine-grained entitlements. For example, customers who invested in developing detailed SAP role models can automate provisioning down to the SAP role level. Unlike traditional identity management systems, CA Identity Manager leverages these roles directly out of target systems instead of requiring redundant definition of each SAP role in CA Identity Manager.

Policy Enforcement

Business policy enforcement often requires custom coding to support your local, unique needs. Policy Xpress lets you configure policies that execute your unique, complex business processes without the need for custom code, often within hours, rather than requiring weeks of programming. This helps reduce the costs of internal development and ongoing maintenance and you will no longer be locked into unsupported, aging software. With Policy Xpress, you can quickly and easily respond to organizational changes, without having to manage an entire software development effort.

Password Management

CA Identity Manager includes a comprehensive set of password management services that increase security by enforcing consistent password policies across the organization. These include:

- **Password policies** enforce different password strength requirements for different users, ensuring that sufficiently strong passwords are used to protect critical applications and accounts.
- **Password synchronization** occurs because CA Identity Manager can propagate passwords across target systems, including synchronizing operating system-level password changes back to CA Identity Manager across Windows®, UNIX® and mainframe environments.

Mass Updates

Organizations often need to support massive entitlement changes as a result of enterprise structure changes, such as the merging of business units or acquisition of new companies. CA Identity Manager supports these types of mass changes using a bulk loader service. Changes can be initiated by feeding in an information file where each text line represents a requested change. CA Identity Manager can also apply a common change to many users which match certain criteria, such as applying the same change to all current employees at a certain site.

Software Development Kit

CA Identity Manager Software Development Kit (SDK) includes a set of documented application programming interfaces (APIs) that let you integrate and extend CA Identity Manager capabilities for your specific environment.

- **Task execution Web services** APIs enable third-party applications to remotely submit CA Identity Manager tasks for execution. This capability is used by organizations to embed identity management services into their existing applications that their users are already using.
- **Business logic SDK** is a set of Java™-based APIs that can be used for embedding custom business logic inside identity management policies.
- **Java connector server SDK** is used to develop custom connectors which support provisioning to homegrown applications.

Configuration Management

Config Xpress is a utility that provides system administrators the ability to easily move components between staging environments for simplified configuration management. It also provides a change analysis report that highlights differences between environments as compared to a current and baseline installation. It provides a "push-button" system documentation process that records the many system components for future reference or as a part of a system recovery plan. Config Xpress also provides a convenient and efficient method to display component relationships. For example, it shows which screens are used by specific tasks and which administrative roles grant access to those tasks.

Enterprise-Class Scalability

CA Identity Manager is deployed by some of the largest enterprises in the world, including those which require the highest degrees of scalability and around-the-clock availability. This same level of service benefits not only large enterprises but customers of various sizes, across various industries. CA Identity Manager's flexible, layered architecture has been designed to support enterprise needs, including:

- **Layered clustering** is supported at every CA Identity Manager infrastructure layer, including the CA Identity Manager application, provisioning Server, connector server and repositories. Clustering support addresses high availability as well as load balancing requirements.
- **Component distribution** can be extended horizontally by adding additional machines in a mirrored fashion. Alternatively, the deployment can be extended vertically by dedicating machines to handling specific functions which carry the highest loads.

Strong Security

Because user identities represent highly sensitive information, CA makes continuous investments to help deliver the highest levels of internal product security. This enables the management of users and their access rights across the entire enterprise while maintaining the product security disciplines in accordance with industry best practices. These features include:

- **Cryptography**—CA Identity Manager uses the Advanced Encryption Standard (AES), incorporating proven cryptographic libraries Crypto-J v3.5 and Crypto-C ME v2.0. These cryptographic requirements include encryption algorithms, key sizes and implementation for handling sensitive data.
- **FIPS 140-2 Support**—Federal Information Processing Standards (FIPS) 140-2 is a security standard for the cryptographic libraries and encryption algorithms which help ensure high standards of data security.
- **Data security**—CA Identity Manager secures data at rest and in transit by using secured protocols over all communication channels between components and endpoints. In the majority of cases, this includes usage of standard protocols over SSL such as HTTP over SSL (HTTPS) and LDAP over SSL (LDAPS).

Reconciliation Services

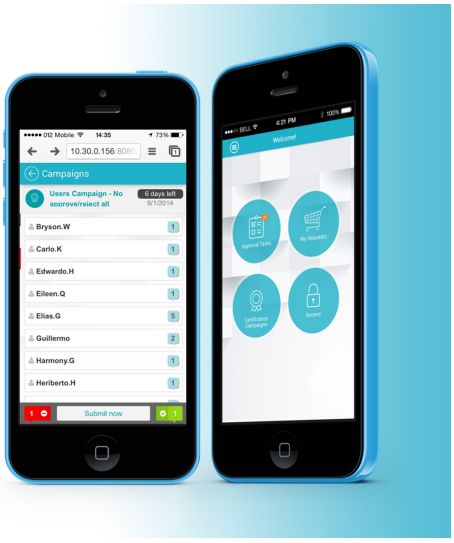
Synchronizing identities and access rights across the enterprise requires bi-directional connectivity with managed systems. Reconciliation services, called Reverse Synchronization, recognize changes made directly on endpoint systems, determine if they are within policy and synchronize them across other systems as appropriate. These include:

- **System acquisition**—Once a new managed system is defined, the reconciliation service discovers the list of existing accounts and automatically maps these accounts to users based on correlation rules. Accounts that do not satisfy correlation rules are flagged as "orphan accounts" for manual review. The system owner can associate accounts to users, mark them as "system accounts," disable accounts or delete accounts.
- **Authoritative system support**—Authoritative systems are business applications or IT platforms designated as the source of certain user or account attributes. CA Identity Manager supports the option to have multiple authoritative systems, each with authority over part of the user population or a subset of attributes. The ability for changes made at authoritative sources to override existing information in CA Identity Manager can be set at multiple levels.

By comparing the known status of accounts in CA Identity Manager with the actual assignment of these accounts in the target systems, Reverse Synchronization discovers when an authorized changes have taken place. Based on this, it can initiate automated alerts or remediation processes such as triggering a manual review by an administrator or initiating reverse actions for these changes.

Mobile Use

CA Identity Suite includes a native mobile application that extends commonly used features of CA Identity Manager to the mobile environment. The mobile app provides the business user with the ability to review and approve workflow requests, perform password self-service operations and review profile details all from a smartphone. This important capability allows the organization to support BYOD policy, and to improve efficiency, responsiveness and user satisfaction while reducing security risks.



Manage identities and entitlements on the go.

System Administration

CA Identity Manager includes a comprehensive set of capabilities that enable you to define what business operations each user can perform and under which business restrictions. This enables you to regulate "who can do what to whom." Delegation models are based on combinations of roles and rules and can include custom logic for modeling unique delegation logic as needed.

- **Workflow-based delegation** provides the ability to easily create and apply approval processes so users can feel confident their actions will be appropriately delegated. Each approval can, in turn, be subject to delegation, allowing approvers to further delegate or transfer approval authority if it was improperly assigned.
- **Granularity of delegation** capabilities (create user, approve access request or view system report) can be defined based on user or organizational attributes or a combination of both.
- **Scoping** defines what specific actions individual users are authorized to perform but also includes the ability to define dynamic, instance-specific rules. For example, a user can have scope over "all users in sales" or "all users at my location."

Auditing and reporting

The CA Identity Manager audit service captures a complete trail of business changes, provides ad-hoc query capabilities and can integrate third-party security information and event management (SIEM) solutions for cross-domain forensic and reporting analysis. In addition, CA Identity Manager reporting services offer the following capabilities:

- **Enterprise-class reporting**—CA Identity Manager includes an embedded version of Business Objects Crystal Reports XI. This scalable approach enables organizations to build customized reports which support enterprise requirements.
- **Snapshot warehouse**—Organizations can periodically schedule capturing of current organizational access policy and actual entitlements assignments. The recorded information is stored in a relational database as an individual snapshot, representing the status at a particular date. Viewing the progression of snapshots stored in the warehouse provides a historical view of access assignments. This information can be used in a forensic scenario to produce reports of assignments at a particular date or for trending to show the evolution over time and provide visibility into gradual changes happening in the organization.
- **Out-of-box reports**—CA Identity Manager includes a set of prebuilt reports that provide valuable visibility into the identity management operation and efficiency through entitlements, policies and workflow insight.

Section 3:

Benefits of a Business User-Centric Approach to Identity Management

The identity management capabilities of the CA Identity Suite enable organizations to quickly provision users to a broad range of applications, to simplify and streamline identity management processes, to enable convenient self-service and to reduce overall security costs. The solution offers also provides capabilities and benefits not available in other solutions, such as:

- **Intuitive, business-oriented user experience**—The user experience and convenience offered by the CA Identity Suite is unmatched in the industry. Key identity management capabilities such as provisioning, self-service, access requests and entitlement management are available in an intuitive, business-oriented experience. The result is improved user satisfaction and increased productivity.
- **Reduced total cost of ownership (TCO)**— Deployment Xpress enables you to get up and running with common identity use cases in a fraction of the time it usually takes with other solutions. Connectors to custom applications can also be deployed easily using Connector Xpress. Our customers have found that deployments are simpler, quicker and require less ongoing code maintenance.
- **Strong, robust connectivity with target systems**—CA Identity Manager includes connectors that provide deep functionality, rather than simple connectivity. For example, the Active Directory (AD) connector enables management of groups and distribution lists directly, simplifying management of AD user information.
- **Proven consumer-scale**—CA Identity Manager is being used today in some of the largest and most complex IT environments in the world. It can meet your needs for scale now and into the future.
- **Integration with other identity capabilities**—CA Identity Manager delivers integration to other identity and access management solutions from CA Technologies, including CA Identity Governance, CA Single Sign-On and CA Advanced Authentication, which improves management of your users and their access to your IT resources and simplifies compliance efforts.

Connect with CA Technologies at ca.com

CA Technologies (NASDAQ: CA) creates software that fuels transformation for companies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with companies worldwide to change the way we live, transact and communicate – across mobile, private and public cloud, distributed and mainframe environments. Learn more at ca.com.

CS200-230039_1016