

Help strengthen security by building a trusted identity environment



Highlights

- ***Build a trusted identity environment by establishing solid identities, using strong credentials and reinforcing identity usage***
- ***Increase efficiencies and help ensure the safety and security of citizens and workers***
- ***Leverage a framework that brings together a common and comprehensive collection of identity processes, workflows and technology***
- ***Integrate identity management into all physical and online processes***

Interactions between individuals and governments have evolved with a dependency on the integrity and strength of identity credentials. Yet recent events involving fraudulent driver's licenses, Social Security cards and travel documents have proven that the trust assumed in the systems which produce these credentials are not justified. Not surprisingly, individuals are concerned with protecting their identities as citizens, employees and consumers. The risks associated with credential abuse are inhibiting organizations, including customs, border management and law enforcement, from reaching consumers, employees and constituents in new ways.

To address these concerns, countries are passing legislation to address the challenge of establishing more secure identities, including the European Union with their agreement to adopt biometric identity cards by 2010. Across the globe, there is a growing comfort with and use of biometrics between governments—and between the public and private sectors. These trends are changing the nature of identity management from discipline-specific and technology-driven to business-oriented, collaborative and process-driven.

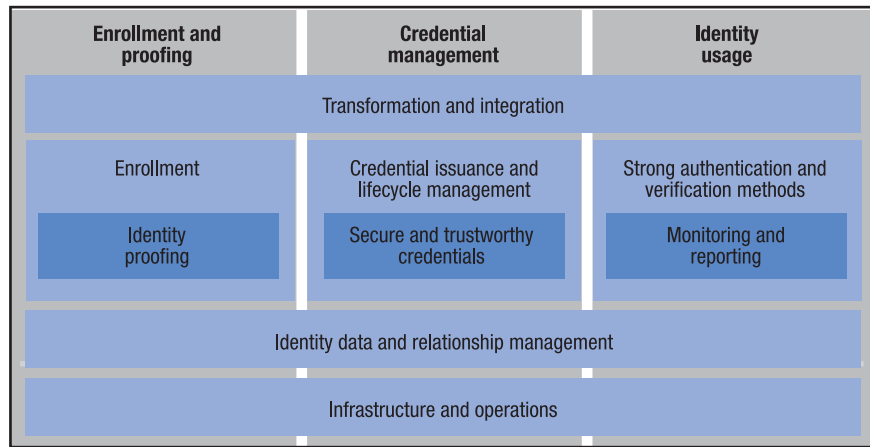
Identity: the state or fact of remaining the same person under varying aspects or conditions.

For organizations managing land, sea and air borders, the massive increase in border crossings and the increased level of threats call for stronger security, processes and information-sharing between border agencies, law enforcement and customs authorities. As our culture becomes more global, the need for identities is even more present. Today's communities, which encompass both the public and private sectors, are broad and complex, and virtual identities are exchanged around the world. In balancing a need for more stringent security controls while keeping countries "open for business," border control agencies must ensure the secure identification of people crossing borders, while maintaining an efficient and cost-effective traffic flow. IBM is helping organizations make this a reality.

Trust: reliance on the integrity, strength, ability, surety, etc., of a person.

Build effective trusted identity systems

Traditionally, many different identity technologies have been implemented, often as stand-alone systems, but these islands of information are inadequate to address the identity challenges of today and the future. Customs, border management and law enforcement



IBM has designed a framework to address trust in human identity systems, to help improve the trustworthiness of identity systems, simplify their complexity and enable new and enhanced business services.

organizations must develop systems that enable collaboration between all stakeholders while integrating the data and processes of their organizations.

The interplay between identity processes and technology, societal boundaries and the business environment is stronger in identity systems than in most other systems. To improve trust in identity systems, organizations must realize that human identification is a universal and general-purpose business function that crosses industry and geographic boundaries. It requires:

- *Maintaining a focus on the full life cycle of identity from initial application through transactional use.*

- *Establishing more robust and reliable entity enrollment and establishment mechanisms.*
- *Employing secure and capable identity credentials.*
- *Using stronger identity authentication and verification mechanisms.*

Trusted identity systems collect and verify identity information from prospective members, allowing you to establish more trustworthy relationships that are instantiated and supported by one or more identity credentials issued in a trusted environment and managed throughout the life cycle of the relationship. Establishing a trusted identity system enables you to increase efficiencies, reduce risk and add new, innovative services.

IBM, a market leader in traditional identity management, has designed a framework to address trust in human identity systems to help meet the identity management need of customs, border management and law enforcement organizations. The IBM approach to trusted identity aims to improve trustworthiness of identity systems, simplifying their complexity and enabling new and enhanced business services, helping you:

- *Improve the trustworthiness of the processes and technologies that make up identity systems.*
- *Integrate the identity life cycle by providing middleware to manage and simplify the life cycle of trusted identities.*
- *Unlock business value by enabling a wide range of identity business process re-engineering and innovation.*

Use service oriented architecture (SOA) to enhance trusted identity systems

Commercial innovation, especially SOA, offers an accelerated route for customs, border management and law enforcement organizations to reap the benefits of implementing a trusted identity solution. SOA is an approach to designing and building information systems that deconstructs applications into separate “services” that are then made available to users as needed.

Because the services are independent of the computing platforms on which they run, they can be consumed independently or linked in different ways to perform a simple or complex function. SOA's inherent flexibility enables organizations to easily connect or add new services to meet evolving operational needs. SOA uses services to connect identity information “silos” with open architecture-based integration, providing access to a variety of legacy systems without alteration. As a result, SOA facilitates integration while leveraging your existing investments.

Because the events that occur today may dictate whom customs, border management and law enforcement organizations need to collaborate with tomorrow, an architecture that supports rapid integration and information sharing with partners is essential. SOA, which provides this flexible architecture, is at the heart of the IBM trusted identity approach.

IBM can help:

Establish more solid identities

Your relationship with constituents begins the second they initiate an identity with your agency. The IBM strategy is to begin building an environment of

trust by incorporating stronger identity establishment and confirmation mechanisms, so identities can be more highly assured.

Use stronger credentials

The pitfalls of having weak password technology are well known. By leveraging stronger identity credentials that are tamper-resistant and harder to copy or forge, and management capabilities that promote greater levels of privacy, transparency and user control, your agency can combat this issue. The framework designed through the IBM trusted identity approach is designed to help agencies select and manage the correct technology, including biometric technology such as fingerprinting or iris scans, smart card technology, and/or near field communications.

Reinforce identity usage

It is critical within a trusted identity environment to know that citizens “are who they say they are.” The IBM trusted identity approach proposes to improve trust in identity usage by applying more robust authentication and verification mechanisms to ensure that identities are used properly across physical and online processes, and to ensure identity termination once the citizen's relationship with your agency has ended.



Leverage a comprehensive trusted identity strategy

The time has come for customs, border management and law enforcement agencies to leverage a new framework that brings together a common and comprehensive collection of identity processes, workflows and technology that is shared by most identity systems. By applying this strategy, you are better able to increase efficiencies without compromising security. For example, you are better positioned to:

- *Quickly verify and authorize identities through more secure identity systems.*
- *Offer new online services to citizens.*
- *Replace paper and manual application processes with a trusted transaction from a quick biometric scan, smart card or near field communication.*
- *Leverage partnerships with other agencies for value added services and capabilities.*
- *Improve compliance posture with stronger audit trails.*
- *Leverage automation in processes and deploy workers in other mission-critical areas.*

Establishing a true trusted identity environment better positions agencies to generate confidence among citizens and to strengthen their compliance posture.

Work with the trusted identity experts

By strengthening each stage of the identity life cycle, you are better able to employ a secure, comprehensive method of building a true trusted identity environment. With their full range of consulting, design, implementation, and management solutions, IBM is empowering customs, border management and law enforcement agencies to unlock business opportunities and better serve their consumers, employees and constituents in safe and secure ways.

For more information

To learn more about how to build trusted identity into your organization, please contact your IBM representative or IBM Business Partner.

© Copyright IBM Corporation 2008

IBM Software Group
Route 100
Somers, NY 10589 U.S.A.

Produced in the United States of America
September 2008
All Rights Reserved

IBM, the IBM logo, ibm.com, Rational, Tivoli and WebSphere are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol (® or ™), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at ibm.com/legal/copytrade.shtml

Other product, company or service names may be trademarks or service marks of others.

Disclaimer: The customer is responsible for ensuring compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the reader may have to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer is in compliance with any law or regulation.



Recyclable, please recycle.

IBS03003-USEN-00