Identity Integration:
An Intuitive Perspective

Background

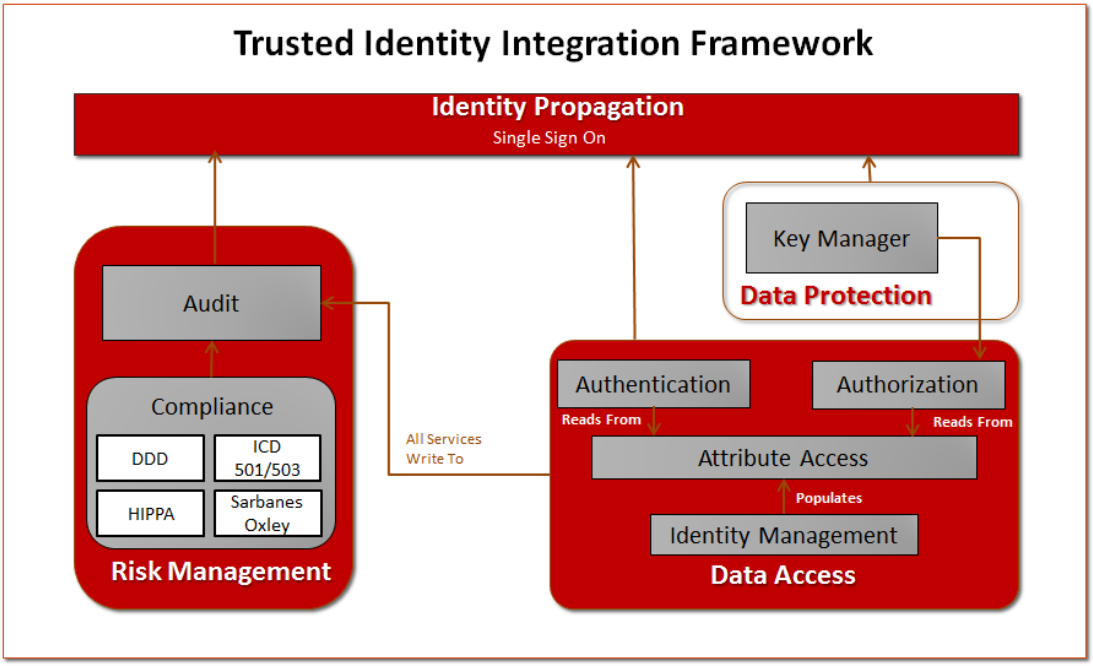
Government agencies and corporations face the dynamic tension to maximize the value of their resources while minimizing the risk of exposure to unauthorized entities. Securing information is vital and critical to any organization's mission requires to effective management of identities, resources and access policies to ensure protected resources are accessed by authorized users and system.

Establishing Trust

The solution consists of a collection of functions referred to collectively Trusted Identity and Integration Framework (TIFF). The TIFF architecture consists of seven major functional identity and access management (IdAM) components: Authentication, Authorization, Identity Management, Attribute Access, Key Management, Identity Propagation and Auditing as illustrated in figure one. Identity and access management (IdAM) is the process where technology and business merge to provide the functionality and processes required to ensure the assets of the enterprise are protected. IdAM solutions validate who you are, what you have access to and tracks where you've been and what you've done. The goal of an IdAM system is to manage and record digital identities, including people, systems, servers and networks and their associated access permissions which permit or deny access to corporate information. Combining identity management, authentication, authorization and auditing functionality into a cohesive, integrated infrastructure provides an enterprise strategy that improves productivity, ensures the protection of corporate resources and reduces IT costs.

Identity Integration

Effective IdAM implementations that include processes, technologies and policies can lower security costs by increasing the efficiency and consolidation of identity management and access control functions into a set of enterprise level security services. Implementing IdAM functions into an integrated set of reusable and centrally managed services decrease the risk of data spills while permitting employees and partners' greater access to corporate resources. In addition to protecting resources, TIFF introduces the use of analytical tools and procedures as a set of services that provide a higher level of regulatory compliance by continuously monitoring



intuitive.it
FOCUSED SOLUTIONS

audit logs that contain events and outcomes as captured by each component in the architecture.

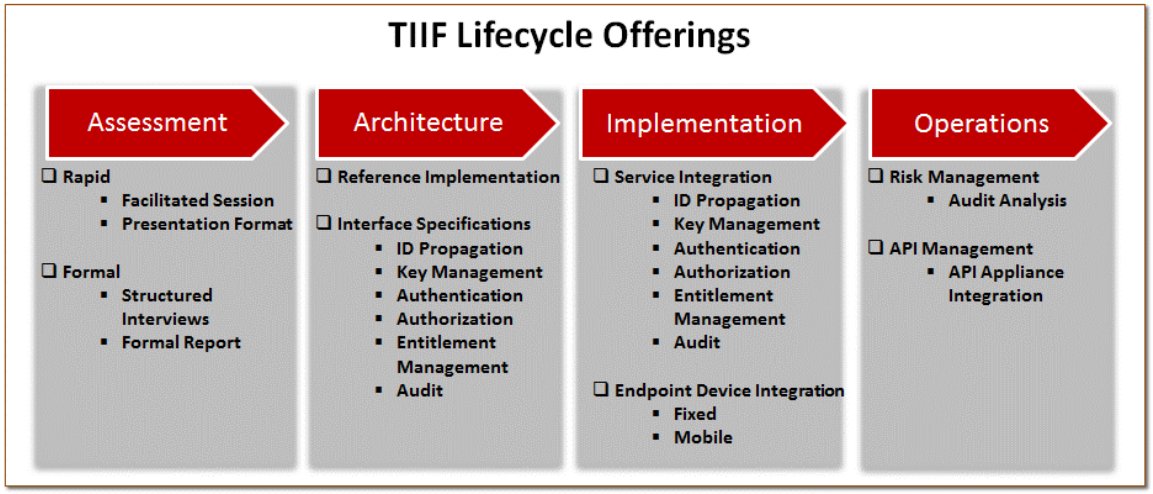
The Framework

The Trusted Identity Integration Framework avoids the complexity and risk of a wholesale change of identity services by using an interface strategy. The TIIF follows a 4-stage lifecycle that reduces risk and complexity.

- *Assessment*—determining the current state of identity integration leveraging the Identity Credential and Access Management (ICAM) Maturity Model.
- *Architecture*—the development of a reference implementation of the architecture to demonstrate and refine capabilities. Documentation of the interface specifications should be completed to allow for parallel development.
- *Implementation*—the interface driven approach allows for service integration in a logical priority order, established in the Assessment Phase.
- *Operations*— continuous monitoring for risk management and Application Program Interface Integration as required.

Conclusion

Integration of identity services with an interface strategy offers a low-risk approach that allows the prioritization of identity service implementations through an integration framework. This interface strategy approach keeps the focus on the information exchange between identity services, vice the complexity of the services themselves.



Contact

12930 Worldgate Dr., Suite 300
Herndon, VA 20170
571.346.3000
info@intuitive.it