



Best Practices for Credential Management

Optimizing Security in Enterprise
Encryption

Ingrian Networks

475 Broadway, Redwood City, CA 94063

Phone 650.261.2400

Toll-free 866.INGRIAN

Fax 650.261.2401

www.ingrian.com

Managing Credentials

Overview of the Problem

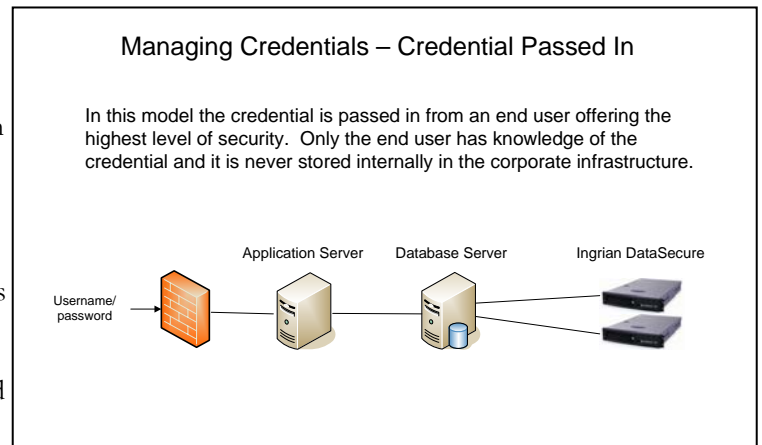
When deploying a solution in which cryptographic keys are stored in, and never exist in the clear outside of, a secure hardware platform, a question commonly asked is “How does one protect the credentials that are used to access and use the keys within the hardware?” So, although the actual keys to decrypt sensitive corporate information are kept in a highly secure environment, the credentials to perform the actual decryption may not be. One could steal the credentials and have the ability to decrypt sensitive corporate information.

This document outlines a few approaches to effectively managing credentials in an enterprise encryption deployment.

Recommended Solutions

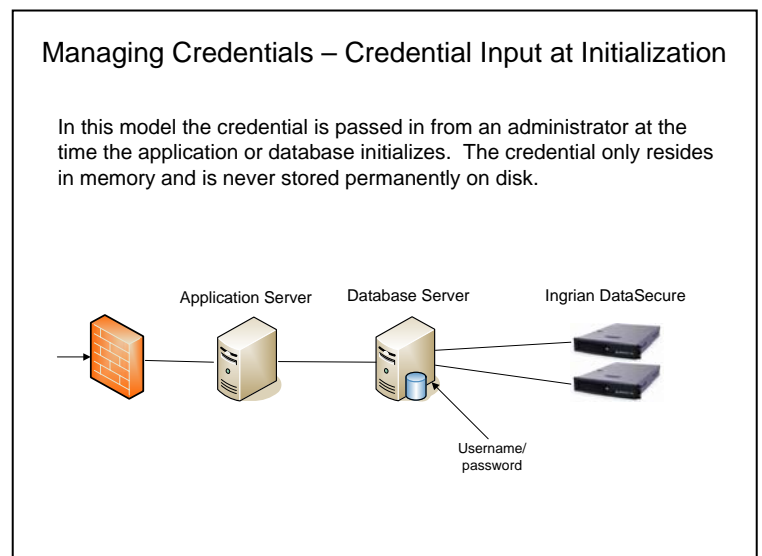
Option #1—Credential Passed In

This approach has the credential passed in from an upstream process. The clear advantage of this approach is that the credential is never stored on disk and therefore cannot be compromised on the machine that is using the credential. The disadvantage of this approach is that we are simply pushing the problem back one level. In the end, the credential will either need to be passed in (i.e. an end user that would presumably provide the highest level of security) or stored on an upstream device such as the Web server. This approach may often be unrealistic since significant application code changes may be required to support this architecture.



Option #2—Credential Input on Initialization

This approach has the credential input at the time the application initializes. The credential only resides in memory and is never written to disk. This approach is viable but may not be practical in situations in which a process or a machine needs to be able to restart automatically without human intervention. This intervention may be unacceptable from a business standpoint.

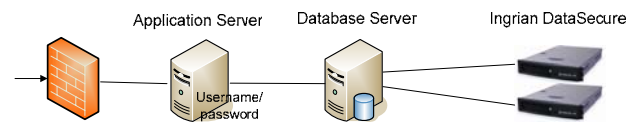


Option #3 (commonly recommended)—Credential Stored Locally and Obfuscated

This approach would have the credentials used to access cryptographic keys reside on a hard disk or similar device. The best approach is to obfuscate the credential in a proprietary way that only the application that is reading the credential would be aware of. A simple encoding mechanism such as hexadecimal or Base64 would be strongly discouraged since this can be easily reverse engineered. A common recommendation is to encrypt the credential with a cryptographic key. While this approach is valuable in providing additional layers of security, the same root problem exists. Where do you ultimately store the key that is used to encrypt the credential? For this reason, it is still recommended to obfuscate the credential (or key) in some proprietary way. One last approach that is commonly recommended is to store the credential in a secure local device such as a smart card. Again, the issue with this approach is the challenge of securing access to the smart card itself. So, if the credential cannot be passed in from an upstream device or provided as user input the generally recommended approach for protecting the credential is to utilize some proprietary form of obfuscation optionally combined with encryption and local security devices. Finally, it is important to enforce minimum (least privileges) access to the credentials using the services available on the host such as file permissions on UNIX environments or registry permissions on Windows environments. Multiple credentials should also be enforced for access to the credentials where possible so that no single administrator can gain access to the credentials.

Managing Credentials – Credential Obfuscated on Disk

In this model the credential is actually stored in the application or database server obfuscated and optionally encrypted.



About Ingrian Networks

Ingrian Networks brings complete data privacy to the enterprise. With Ingrian DataSecure Platforms, organizations can protect critical data from both internal and external threats, and ensure compliance with legislative and policy mandates for security. DataSecure features a dedicated security appliance and specialized software that enables organizations to encrypt critical data in applications and databases. With its capabilities for granular encryption, seamless integration, and centralized security management, DataSecure enables organizations to guard against a range of security threats, with unparalleled ease and cost effectiveness. Ingrian is a privately held company backed by such investors as Globespan Capital Partners, HighBAR Ventures, Menlo Ventures, Partech International, and Prism Venture Partners. For more information, visit www.ingrian.com.

© Copyright 2006 Ingrian Networks. The Ingrian Logo, Ingrian, and DataSecure are registered trademarks of Ingrian Networks. All other brand names are trademarks of their respective holders.