

# Whitepaper: Credential Management

By Kai Cheung, VP Architecture, Echoworx

October 2011

This paper will provide an overview of credentials and credential management, as well as outline how credentials are used on data networks and mobile devices and a technology approach for managing them.

## **INTRODUCTION**

The proliferation in usage of mobile devices for business is creating significant security concerns for IT managers. The challenges posed by mobile workers are many. Not only are they increasingly accessing business applications and corporate information from outside the firewall, more and more sensitive data is being transmitted and stored using public networks and cloud-based services. As recent breaches have shown, the security measures available for public Internet or cloud services have proven to fall short of the mark in terms of securing corporate data.

Mobile workers themselves also present challenges, since they often conduct business communications without a working knowledge of corporate policies and security practices. In addition, the portability of devices puts data at risk in the case of loss or theft. Analysts estimate that anywhere from 20 to 25 per cent of devices are lost or stolen.

To mitigate risk, organizations are turning to measures such as remote wiping of content as a stop-gap measure, but it also has limitations since signals to the devices can be blocked, and there could be substantial delays before the action can be carried out. Securing devices at the endpoint has also been fraught with difficulties, since solutions are typically specific to operating systems such as BlackBerry, iOS and Android, and do not provide the capability to centrally manage over-the-air content.

Within enterprise ranks, securing content access, delivery and storage is well in hand. Typically it is done through the application of credential management tools leveraging a public key infrastructure (PKI) platform. However, until recently, this capability has not been a viable option for mobile simply because the devices are not tied to the corporate network. Piecemeal attempts have been both costly and cumbersome to manage, as well as overly complicated for users.

The time has come for an efficient mobile endpoint solution to tackle the myriad of mobile and cloud security challenges. Rather than investing in a comprehensive and costly PKI infrastructure however, organizations, as well as developers, can now turn to third party platforms to meet their credential management needs. By "plugging into" a full PKI infrastructure that operates the digital certificates for them, developers can eliminate the high costs associated with credential management, while applying the needed security measures across multiple applications and platforms.

## **CREDENTIALS EXPLAINED**

Secure sign-on and encryption policies are putting credential management – and in particular public key infrastructure (PKI) – under closer scrutiny these days. In fact, data encryption and credential management for mobile users is becoming the number one

priority for enterprise IT managers and mobile application developers as they face a growing need to extend authentication processes to enable secure sign-on and encryption from any device.

Recent breaches have shown that password protection is simply not enough as organizations deal with increasingly stringent legislative demands for authentication. Even so-called encryption features in mobile devices can easily be bypassed, and are proving to be tantamount to locking a door and leaving the key under the mat for others to break in. Given the costs and complexities of PKI deployment however, application of credential management to mobile devices has been problematic.

By way of explanation, a credential is a proof of authority or qualification. Common examples are government-issued identification documents, documents for government services such as a health card or library card, security clearances, user names and passwords, etc.

To demonstrate a person's entitlement of authority or qualification, the holder of a credential is usually asked to present the appropriate documentation or secret knowledge i.e. passwords or keys. Credentials must be easily verifiable and difficult to forge or replicate. In the offline world, that would be the equivalent of having to present photo identification from an acknowledged authority (e.g. Department of Motor Vehicles) to pick up a registered letter.

In the online world, a valid credential must meet the following criteria:

1. It must be issued by an appropriate certificate authority such as a government ministry, school, institution, and/or system administrator
2. The enrolment and verification of the credential holder must be carried out by the appropriate registration authority
3. It must not have expired, or been altered, replicated or reported stolen
4. It must be able to be verified by the appropriate Certificate Authority (CA)

Credential management goes hand-in-hand with cryptography, a process used to keep information safe. Modern cryptography relies on the use of encryption/decryption keys and algorithms that make it impossible for anyone but the credential holder to access that information.

Private key cryptography uses symmetric keys to encrypt/decrypt information. As such it requires a pre-sharing agreement between the sender and the recipient.

Public key cryptography on the other hand allows for the secure exchange of symmetric keys between the sender and the recipient, to allow for the sending and receiving of encrypted information without a pre-sharing agreement. The sender's "signature" on the information can then be verified by the recipient.

In public key cryptography, public keys are usually distributed in the form of a digital certificate. A digital certificate is a type of credential usually issued and digitally signed by a widely-trusted Certificate Authority. The Certificate Authority validates the bond between a public key and the identity of the subject key owner (principal); and is responsible for verifying the identity of the owner of the public key and assuring proof-of-possession of the associated private key before a certificate is issued.

Below is a comparison between private-key and public-key cryptography:

	<b>Private Key Cryptography</b>	<b>Public Key Cryptography</b>
Key Length required to secure information	Shorter (256 bits is the currently accepted standard)	Longer (2048 bits is the currently accepted standard)
Encryption / Decryption Speed	Faster	Slower
Key Distribution	Difficult to manage, since symmetric keys must be pre-shared	Easier to manage, since public keys are distributed or generated on public servers
Digital Signature	Not supported	Supported

Public key cryptography is only secure as long as the keys can be trusted. A PKI is the collection of entities (individual persons, machines or services – including certification authorities, certified subjects and relying parties), policies and technologies that define the scope of a trust domain in which public keys are used.

The common standards for PKI technologies are:

- Digital Certificate: X.509 certificate
- Email encryption and signing: S/MIME
- File encryption and signing: RSA on signature and encryption keys
- Secure web protocol: HTTPS / TLS / SSL
- Identity-based encryption (where digital certificates are optional)

Digital certificates are widely deployed by businesses. However, with vendor-provided PKI solutions, infrastructure costs are high, and implementation and management requirements extensive. This can preclude many organizations from adopting PKI platforms, since they lack the necessary IT resources.

## **MANAGED PKI**

To help reduce complexity and costs, organizations can now leverage a fully-managed, software-as-a-service (SaaS) credential management service that can provide the following capabilities.

- Key Services to manage the digital certificate lifecycle, including creation, rollover, revocation, and expiry.
- Trust Services that provide a digital certificate lookup for verifying digital signatures.
- Administration Services to manage the entire trust hierarchy, up to the Root Certificate Authority.

A fully managed SaaS-based credential service allows businesses to reap the full benefit of credential management at a much lower cost. Now available and ready for the market, this service supports a Single-Sign-On (SSO) framework, which requires users to authenticate only once with their credentials for web services and applications. This can easily be extended to mobile, by installing password-protected digital certificates directly on devices. In the event of a breach of any kind managers can immediately revoke or suspend the user’s credentials through a central console without having to get physical access to the device, ensuring no one can read its content.

In this model, businesses running enterprise applications on mobile devices can also use the service to secure sensitive information stored locally and uploaded to data clouds such as

Box.net and iCloud. This enables them to secure their data anywhere without having to trust third-party cloud providers to protect it. Independent software vendors can also implement applications that will take advantage of SaaS-based credential management to assure their users that data is secured for them, by them.

## **CONCLUSION**

The benefits of PKI in managing mobile and cloud security are becoming increasingly evident. Through a fully-managed approach, organizations can eliminate the costs and complexities of an in-house PKI infrastructure, while centrally controlling access to and usage of sensitive business documents.

As the escalation of mobile devices and cloud-based applications for business usage grow, the need for more stringent, manageable security measures is paramount. Given the scope of the challenge, it is incumbent on enterprises to extend their credential management activities beyond the walls of the enterprise. This entails applying new technology approaches that are flexible, secure and easy to manage.

## **ABOUT ECHOWORX**

Echoworx Corporation is the leading provider of managed encryption services for complete enterprise email and data protection.

Echoworx provides an API infrastructure for credential management and allows third parties to integrate our credential management functionality into their applications. This is useful for organizations looking to issue valid and verifiable credentials without having to manage PKI and digital certificates in-house. As a managed encryption service provider, Echoworx hides the complexities of credential management while providing users with a web-based console for easy credential management.

This console allows the administrator to easily perform basic functions such as adding, removing or suspending users, as well as advanced functions such as revoking user credentials. Having SaaS-based Credential Management accessible through a web service API allows businesses to also leverage and manage digital certificates on mobile devices and web applications. APIs provided by Echoworx are completely web-standards based, fully documented, and accessed using common protocols, including HTTP, HTTPS, XML, and JSON.

For more information: [www.echoworx.com](http://www.echoworx.com)

## **ABOUT THE AUTHOR**

As Vice President of Architecture, Kai Cheung manages the Echoworx Security Suite, Encrypted Mail Exchange and Encrypted Mail Gateway product lines.

Prior to joining the Echoworx team, Cheung had accumulated over 20 years experience in the computer software industry working in ISP billing systems and architecting multi-million dollar systems for the Ontario Public Service. Recently Cheung was CIO with iGO International Inc., where he led the company's product architecture for Wireless Incident Management Systems.

Cheung has an Honours Bachelor of Mathematics from the University of Waterloo, with a double major in Computer Science, and Combinatorics and Optimization.

Kai can be reached at: [cheung@echoworx.com](mailto:cheung@echoworx.com)

### **References**

Public Key Cryptography Standards (PKCS)

<http://www.rsa.com/rsalabs/node.asp?id=2124>

DES / Triple DES standard:

<http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf>

AES / AES-256 standard:

<http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

TLS Protocol Standard v1.2:

<http://tools.ietf.org/html/rfc5246>