The Race to Secure the Cloud 2.0

How Best Practices in Cryptography and Key Management Will Create Competitive Advantage When Securing the Cloud

First one to secure Cloud 2.0 wins.

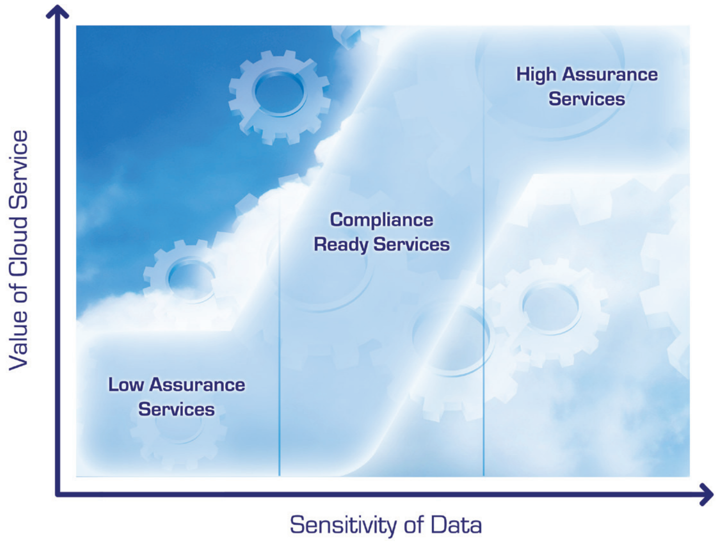
The Cloud, it seems, is everywhere these days.

From consumer offerings like Apple's iCloud to Google Docs and enterprise offerings like Salesforce.com, Amazon EC2 and Rackspace, the Cloud is the most hyped development in IT since the advent of the Internet.

And while the Cloud isn't necessarily a technology revolution, there's no question that it does represent a major change in the business model for IT delivery.

The first phase in that new business model has been defined by a variety of services that entice organizations to move relatively low-risk data to the Cloud. The benefits are significant: cost-savings, greater agility and on-demand capacity. The competition in this phase continues to be fierce, with new providers fighting to build a brand and traditional vendors defending their patch and hedging their bets.

But the next phase of the business model – what some have called Cloud 2.0 – will be about making money. Enterprise customers and service providers alike are strategizing to see how they can move beyond commodity services to drive profit from the Cloud and use it for competitive advantage – increasing the value of the services on offer, making them an indispensable part of IT landscape.



One of the primary challenges, of course, is security. Most companies aren't yet convinced that the benefits of the Cloud outweigh the risks[1]. Enterprises and governments are certainly attracted to the prospect of even greater savings by using the Cloud for storage and processing of their more sensitive data – after all, it is these business-critical activities that are harder and more costly to manage and so the savings can be greater. But faced with privacy mandates and escalating compliance obligations they're not sure who to trust to secure these high-value and high-risk assets.

The questions reverberate throughout the business community and the security industry: How do you secure the Cloud? What digital assets or business processes can be safely moved to the Cloud? What's the appropriate threshold of security for payment information, for example? How about medical records? What will it take to protect corporate brands and even national security? And who's going to accept the liability for failure?

There's certainly no silver bullet but it seems inevitable that at the core of any security architecture there will be a reliance on cryptography. Just as the industry turned to cryptography as the best way to build confidence around

[1] ISACA – IT Risk/Reward Barometer (March 2011)

Internet commerce and to secure the global payments network, cloud-based services providers will find cryptography to be the best way to prove they can be trusted to deliver the confidentiality, system integrity and accountability their customers will demand.

The stakes are extremely high. The companies and service providers that are first to crack this nut stand to gain tangible competitive advantage and realize significant benefit to their bottom line.

What are the risks that are holding us back?

It's all about control – or rather, lack of it.

A key premise of the Cloud is based on saving money and gaining flexibility by sharing resources such as storage, networks, servers and applications with other organizations. Sharing resources necessarily means losing some control. And depending on the types of cloud services being used, organizations today may fear they are giving up just too much control of their critical data assets.

Clouds rely on shared resources – and that means giving up some control

Of the many threats posed by cloud computing, four general issues are repeatedly highlighted by independent bodies such as the Cloud Security Alliance[2]:

1. **Data leakage.** The very nature of cloud computing makes it harder to track the flow of data and more vulnerable to inadvertent exposure. Distributed computing and storage creates a viral data footprint throughout the Cloud, across the networks over which it travels and in the residual copies of that data that linger long after the service is no longer in use.

2. **Shared technology.** Much of the technology used to build clouds has an enterprise pedigree and may lack the ability or not be properly architected to provide the strong isolation and segregation necessary for a truly multi-tenant environment. Attackers can exploit shared technology loopholes to hijack accounts, peer over the information barriers and gain unauthorized access to other cloud customers' data.

3. **Malicious insiders.** Clouds can take the insider threat to a new level. Organized crime, corporate spies or even nation-state sponsored intruders can make mischief and even unwitting insiders provide an entry mechanism for Advanced Persistent Threats.

4. **Unknown risk profiles.** The Cloud's inherent lack of transparency makes it hard to quantify risk. No matter how secure some links in the chain may be, it's hard to determine liability and accountability without demonstrable security, end-to-end. Without shared trust it's difficult to agree who's 'watching the store'.

To win business as the Cloud gets serious, service providers must convince their customers they are serious about these security concerns and can be trusted to safeguard data and enforce segregation between the various tenants in a shared system.

The key to winning trust in the Cloud is to make control a tangible commodity – something that can be assessed and quantified, enabling customers to satisfy the same security audits, demonstrate regulatory compliance and fulfill the same SLAs they do today. The business model might change but the rules of the road don't.

To win business as the Cloud gets serious, providers must be trusted to safeguard data

[2] Top Threats to Cloud Computing V1.0, prepared by the Cloud Security Alliance, March 2010

Cryptography: the key to securing the Cloud.

To put it plainly, there is no more widely proven and generally accepted method to secure the Cloud than cryptography. And there are no cloud service providers that can successfully offer secure services without employing cryptography broadly across their service infrastructure.

Cryptography is a core technology that can be applied in various ways to achieve unique benefits. Most commonly, cryptography is the science behind encryption, the process of rendering data unreadable to all but authorized users, and therefore useless in the event of a data breach. Secondly, cryptography can be used to create digital identities and credentials that can be used to strongly authenticate users, devices and applications. And thirdly, cryptography is used to create digital signatures that are used to establish authenticity and integrity. Applied individually or together, these techniques provide solutions for many of the major threats to cloud security.

Ultimately, cryptography is ideally suited to securing the Cloud because:

1. **It focuses on protecting data itself, throughout its entire lifecycle - wherever it might be.** Where other security technologies such as anti-virus, firewalls and monitoring systems protect data indirectly by protecting the IT infrastructure or systems through which it passes, cryptography, and in particular encryption, goes deeper and protects the data itself within the data center, within the Cloud and everywhere in between.

   Think of it like the envelopes we use to seal our letters. We could choose to use only post cards, even for our bank statements, and rely on locks on every mailbox, armor for every mail van and video cameras in every post office to protect our messages from prying eyes. But there would inevitably be gaps, areas we couldn't protect and so we put our letters in envelopes, protecting our 'data' throughout the system. Encryption is the IT equivalent to an unbreakable envelope that protects the data wherever it goes, from sender to receiver, in storage and in use.

2. **Cryptography provides fail-safe protection.** If encrypted data is inadvertently lost, not deleted when required or unexpectedly proliferated, it remains secure because it cannot be read – it is protected by default. Similarly, the use of cryptography to digitally sign software images, messages and commands, audit logs or account details forces a positive validation to occur before any of these systems, instructions or records are trusted.

3. **It offers a measureable proof of security.** A unique strength of cryptography is that it is more than 'best effort' security. Whether it is establishing service segregation, attesting to audit log integrity or enforcing dual controls or separation of duties, cryptography tends to be clear cut . Audits either validate or they don't, data is either readable or it isn't and authorization is either granted or not. There's no middle ground, no room for doubt and it's virtually impossible to break. That means providers can offer evidence of tangible controls to customers and compliance auditors.

Cryptography can help secure virtually every aspect of the Cloud

Where in the Cloud can cryptography help?

Cryptography can help secure virtually every aspect of the Cloud. Here are a few of the most immediate areas where encryption and other forms of cryptography can make a difference.

Network encryption. Data has to move to, from and between clouds. In virtually all cases the network cannot be trusted, and all data (not just the sensitive data) should be encrypted whenever it moves. Whether it's SSL for temporary web connections to and from consumers, or backend interconnects between service provider datacenters, network encryption is a critical layer of protection that can be easily deployed, has minimal impact on performance and remains transparent to end users.

Cryptography provides clear evidence of controls to auditors and customers.

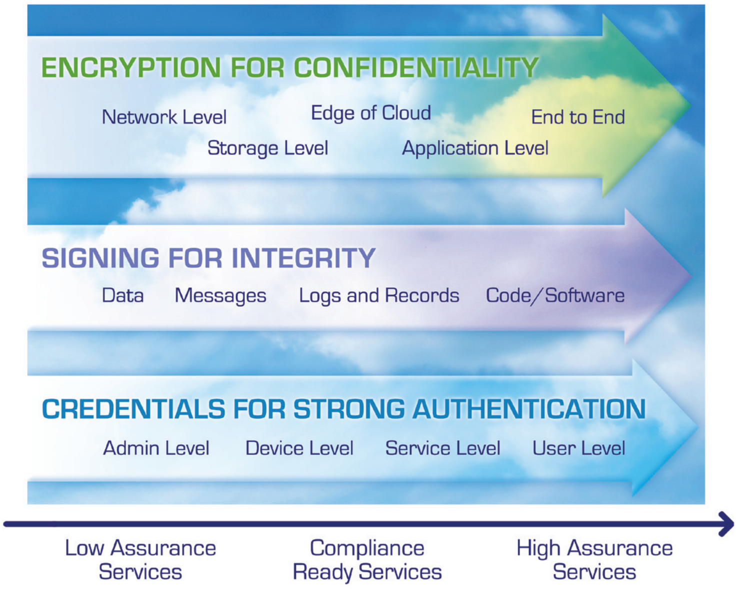
Storage encryption. Any sensitive data stored in the Cloud should be encrypted, whether it's a long-term archive, temporary cache or a live database. Storage encryption can be an easy solution to deploy and is largely transparent, but there are challenges, mostly revolving around key management. Guaranteeing data is available whenever it is needed means keeping encryption keys accessible at all times, especially since notice periods are short in disaster recovery situations.

Application level encryption. Particularly sensitive data should only be exposed on a need to know basis, encrypted as soon as possible and decrypted only when necessary. This selective approach can only be performed at the application level. Developers need access to on-demand encryption and decryption services, specialist policy enforcement and potentially authorization on a per transaction basis. Providers of platform-as-a-service (PaaS) may need to make these capabilities available to developers through existing cryptography APIs to allow the migration of legacy applications.

Edge of cloud encryption. Some cloud consumers will simply not accept that a cloud can deliver confidentiality and will take the matter into their own hands, encrypting sensitive data before it reaches the Cloud as it leaves their domain of control. Cloud providers may choose to provide this service as an extension of their offerings.

Data and message integrity. Data privacy mandates quite rightly focus attention on encryption to provide confidentiality. But security requirements also point to the need to ensure that data is not modified – either maliciously or accidentally. Digital signing, a use of cryptography that creates a digital 'fingerprint' of the document or message, provides a method to validate integrity that is as hard to forge as encryption is hard to crack.

System integrity. While it's important that the customer's data has not been changed, it is equally important that a cloud-based application has not been tampered with. Malware and persistent embedded attacks within applications can be used to circumvent other security measures, potentially even turning off or bypassing encryption. Digital signatures can also prove the integrity and authenticity of application code and software, whether developed by the consumer or by the provider, preventing code that fails validation from executing.



System accountability. As premium cloud services deal with increasingly sensitive data, system accountability will come under greater scrutiny and compliance officers and auditors will require proof. Using strong signing techniques, trusted timestamps and enforced dual controls, cryptography can be used to help ensure that audit logs, event reports and human processes are trustworthy and of evidentiary strength.

Strong authentication. As more valuable data is moved to the Cloud, techniques based on the use of cryptography to create trusted digital identities enable strong authentication that can replace or augment passwords to provide greater security for access by users, approvers and administrators.

Not all cryptography is strong cryptography.

Unfortunately, simply deploying encryption or signing isn't always enough and consumers of cloud services and auditors will be wise to dig a little deeper. Cryptography done well is effectively unbreakable even to the most powerful attacker. But just as some locks prove virtually no match for an experienced thief, cryptography implemented poorly can be easily broken or circumvented by a cyber-intruder.

Cryptography done well is effectively unbreakable, but done weakly creates a false sense of security

At the heart of any system that relies on the use of cryptography is the topic of key management – the processes for protecting, administering and controlling the use of cryptographic keys.

After all, no matter how good the lock is, your security is useless if you leave the key in the door, under the mat or hand out copies to anyone that asks.

Inadequate key management practices and poorly architected systems can easily lead to a false sense of security both for services providers and service consumers, putting brand and reputation in jeopardy.

For service providers who want to earn their customer's trust in the Cloud, the critical points of differentiation will come down to this: how and where are they using cryptography and who's looking after the keys? The answers will need to stand up to scrutiny and, more importantly, pass the test of time.

Best practices matter in the Cloud, too.

Like most technology in the Cloud, encryption and other forms of cryptography are not new. In fact, they have been mandated in regulated industries for years and are virtually the default for protecting everything from stolen laptops to ATM networks to e-commerce transactions.

A number of best practices have become firmly established which mean cloud providers don't have to reinvent the wheel. These tried and tested design approaches can be considered to be 'standards of due care' for any cloud provider that wants to turn their use of cryptography from a business liability into a marketing asset and for any cloud consumer that wants to stay in control. The list, which was developed by Thales e-Security based on practical experience, is not exhaustive but does provide a solid baseline for those assessing cryptographic security.

Thales Standards of Due Care provide a solid baseline for assessing cryptographic security

Standards of Due Care for Cryptographic Security

1. **Know the origin and quality of your keys.** Ensure your random number source is up to international standards. If your encryption keys aren't sound you're making the job of the attacker much easier.

2. **Know exactly where your keys are and who/what systems can access them at all times.** Even if fragments of data are scattered across the Cloud, if you control the keys, you control the data.

3. **Ensure each key is only used for one purpose.** Encrypting data passing between clouds, signing trusted application code, or authenticating service requests should be governed by distinct key management activities. Reuse of keys significantly increases risk.

4. **Formalize a plan to rotate, refresh, retain and destroy keys.** Overworked keys are a liability and obsolete keys are an unnecessary risk.

5. **Only use globally accepted and proven algorithms and key lengths.** Real security is a moving target; sometimes it's good to be in the mainstream.

6. **Adopt independently certified products wherever possible.** Cryptographic programming is hard to get right. If you're tempted to write cryptographic software yourself, you may be jeopardizing your security.

7. **Implement dual control with strong separation for all sensitive operations.** With unbreakable cryptography, the attacker will go after the keys and the people that manage them. Avoid super users and single points of attack.

8. **Ensure your keys are securely backed up and available to your redundant systems.** Cloud security is about availability as well as confidentiality.

9. **Control access to cryptographic functions and systems using strong authentication.** Security relies on consistency; strong keys shouldn't be accessed by weak passwords

10. **Never allow anyone or any 'open' system to come into possession of the full plaintext of a private or secret key.** Theft of a key is an attack that keeps on giving, unscrambling past and future data without detection.

For cloud service providers, these Standards of Due Care are more than just best practices, they are minimal acceptable standards – failure to adhere to them could easily be seen as negligence in the eyes of customers, auditors and regulators. However, implemented correctly, these Standards of Due Care allow service providers to prove they can secure and control higher-risk, more sensitive and regulated data –delivering higher levels of trust and building stronger more valuable relationships between their services and those that consume them.

Thales can help.

While the Cloud is still embryonic, strong cryptography and key management are not – these are well-defined areas of security and have been successful deployed for years. That means cloud service providers can incorporate comprehensive encryption, signing and authentication into their infrastructure with confidence, providing them with a competitive advantage as the race for market share in the next phase of the Cloud plays out.

As you consider the security posture of your current services, the scope of future offerings and how to build out the infrastructure to support them you'll find no better partner than Thales e-Security.

The Thales advantage

Strong track record: Thales has an unparalleled 40 year history in delivering encryption and key management solutions for some of the most demanding security organizations in the World and has been at the center of industry initiatives such as securing the global payments infrastructure and as a founder of the KMIP key management standard.

Partner neutrality: Thales recognizes that encryption, signing and key management can be applied to a wide variety of systems, both commercial products and custom-built applications. We enable these technologies to be hardened at the platform level in an open and standardized way. This equips our customers to support the Standards of Due Care in a consistent manor across their critical infrastructure.

Focus on making it easy: Cryptography can often carry a stigma of complexity and inconvenience and Thales addresses this head-on. Our products focus on simplifying complex key management and automating tasks wherever possible to deliver industry leading scalability. The Thales Security World architecture, for example, provides a framework that maps security policies to a flexible hardware-based security infrastructure and provides for the total lifecycle management of security-critical encryption keys.

Superior product and service portfolio: Thales provides a comprehensive portfolio that enables critical data assets to be protected throughout their lifecycle – when in storage, passing over communications networks and while in use by business applications – all of which are vital aspects of a cloud security strategy. These products are complemented by a best-in-industry partner program to certify interoperability with leading software security vendors and a world-class professional services and consulting team.

We invite you to work with us on comprehensive data protection strategy that follows the Standards of Due Care and as a result can drive significant business opportunities.

About Thales.

Thales e-Security is a leading global provider of data protection solutions. With a 40-year track record of protecting the most sensitive corporate and government information, Thales encryption and key management solutions are an essential component of any critical IT infrastructure. Thales makes it easy to enhance the security of software-based business applications and reduce the cost and complexity associated with the use of cryptography across the organization and out to the Cloud.

Thales solutions include:

- nShield - High assurance Hardware Security Modules (HSMs) deliver the industry's most operationally efficient key management framework and provide a tamper-resistant platform to perform cryptographic operations and manage high value keys associated with digital signing, PKI and encryption for applications, databases, web servers and more.
- Datacryptor - High speed network encryption solutions to secure data traversing networks between data centers and disaster recovery sites.
- payShield - Payment security for online banking, payment transaction and PIN processing, contactless and mobile payments and payment card issuance.
- Encryption Manager for Storage – High assurance key management appliances for storage encryption infrastructure, providing standards-based management of encryption keys on behalf of tape, disk and SAN switches.
- Timestamp Server – Trusted time stamping and signing of messages, instructions, audit logs and other electronic documents to support trusted forensics and nonrepudiation.

Thales enables customers to utilize cryptographic security to enhance their business and satisfy evolving compliance requirements as well as facilitate the secure adoption of new technologies and delivery models including virtualization and cloud computing.

Thales e-Security

Americas: 2200 North Commerce Parkway, Suite 200 • Weston • Florida 33326 • Tel: +1 888 744 4976 or +1 954 888 6200 • Fax: +1 954 888 6211 • E-mail: sales@thalesesec.com
Asia Pacific: Units 2205-06, 22/F Vicwood Plaza, 199 Des Voeux Road Central • Hong Kong, PRC • Tel: +852 2815 8633 • Fax: +852 2815 8141 • E-mail: asia.sales@thales-esecurity.com
Europe, Middle East, Africa: Meadow View House, Long Crendon, Aylesbury • Buckinghamshire • HP18 9EQ • Tel: +44 (0)1844 201800 Fax: +44 (0)1844 208550 • E-mail: emea.sales@thales-esecurity.com