WHITE PAPER: CHOOSING A CLOUD HOSTING PROVIDER WITH CONFIDENCE

WHITE PAPER

CHOOSING A CLOUD HOSTING PROVIDER WITH CONFIDENCE

VERISIGN SSL CERTIFICATES PROVIDE A SECURE BRIDGE TO TRUSTED CLOUD HOSTING PROVIDERS

Now from Symantec. | VeriSign Authentication Services

VeriSign Trusted™

INTRODUCTION

Cloud computing is rapidly transforming the IT landscape, and the conversation around adopting cloud technology has progressed from 'if' to 'when'. Enterprises are showing strong interest in outsourced ('public') cloud offerings that can help them reduce costs and increase business agility. These cloud services offer enormous economic benefits, but they also pose significant potential risks for enterprises that must safeguard corporate information assets while complying with a myriad of industry and government regulations.

Many cloud service providers can deliver the security that enterprises need and SSL (secure sockets layer) certificates are part of the solution. More specifically, SSL is the solution for securing data when it is in motion. The goal of this white paper is to help enterprises make pragmatic decisions about where and when to use cloud solutions by outlining specific issues that enterprises should raise with hosting providers before selecting a vendor, and by highlighting the ways in which SSL from a trusted certificate authority can help enterprises conduct business in the cloud with confidence.

CLOUD COMPUTING: NEW OPPORTUNITIES, NEW SECURITY CHALLENGES

Most organisations cite cost savings as the most immediate benefit of cloud computing. For the enterprise, cloud services offer lower IT capital expenditures and operating costs, on-demand capacity with self-service provisioning and pay-per-use pricing models for greater flexibility and agility. The service provider, in turn, achieves exponentially greater economies of scale by providing a standardised set of computing resources to a large base of customers. Many enterprise hosting providers are already well positioned in the market and have the core competencies (people, processes, technology) to deliver the promise of cloud computing to the enterprise.

Despite the clear economic benefits of using cloud services, concerns about security, compliance and data privacy have slowed enterprise adoption. An IDC survey of IT executives reveals that security is the #1 challenge facing IT cloud services.[1] Gartner Research has identified seven specific areas of security risk[2] associated with enterprise cloud computing and recommends that organisations address several key issues when selecting a cloud hosting provider:

1. **Access privileges** – Cloud service providers should be able to demonstrate they enforce adequate hiring, oversight and access controls to enforce administrative delegation.
2. **Regulatory compliance** – Enterprises are accountable for their own data even when it's in a public cloud and should ensure their providers are ready and willing to undergo audits.
3. **Data provenance** – When selecting a provider, ask where their data centres are located and if they can commit to specific privacy requirements.

Ready or not, here comes Cloud Computing

Some people believe cloud computing is the most significant paradigm shift since the advent of the internet. Others think it's just a fad. But one thing is for certain: cloud technology is quickly rising to the top of every CIO's priority list.

– Source: Gartner EXP Worldwide Survey (http://www.gartner.com/it/page.jsp?id=1283413)

Organisations are accelerating their uptake of cloud services and industry analysts such as Gartner Research estimate that enterprises around the world will cumulatively spend USD $112 billion on cloud services over the next five years.

– Source: Gartner Research (http://www.gartner.com/it/page.jsp?id=1389313)

1. Source: IDC eXchange (http://blogs.idc.com/ie/?p=730)

2. 'Assessing the Security Risks of Cloud Computing' (http://www.gartner.com/DisplayDocument?id=685308) Gartner, 3 June 2008.

4. **Data segregation** – Most public clouds are shared environments and it is critical to make sure hosting providers can guarantee complete data segregation for secure multi-tenancy.
5. **Data recovery** – Enterprises must make sure their hosting provider has the ability to do a complete restoration in the event of a disaster.
6. **Monitoring and reporting** – Monitoring and logging public cloud activity is hard to do, so enterprises should ask for proof that their hosting providers can support investigations.
7. **Business continuity** – Businesses come and go, and enterprises should ask hard questions about the portability of their data to avoid lock-in or potential loss if the business fails.

To reap the benefits of cloud computing without increasing security and compliance risks, enterprises must ensure they work only with trusted service providers that can address these and other cloud security challenges. What's more, when enterprises move from using just one cloud-based service to using several from different providers, they must manage all these issues across multiple operators, each with different infrastructures, operational policies and security skills. This complexity of trust requirements drives the need for a ubiquitous, highly reliable method to secure your data as it moves to, from and around the cloud.

SSL IS THE KEY TO SECURE CLOUD COMPUTING FOR THE ENTERPRISE

SSL is a security protocol used by web browsers and web servers to help users protect their data during transfer. SSL is the standard for establishing trusted exchanges of information over the internet. Without the ubiquity of SSL, any trust over the internet simply would not be possible. SSL comes into play anytime data changes location. If an enterprise keeps its data in the cloud, secure network access to it is important. Plus, that data is likely to move around between servers in the cloud when the service provider performs routine management functions. Whether data is moving between server and browser or between server and server, SSL helps to secure it.

SSL delivers two services that help solve some cloud security issues. First, SSL encryption keeps prying eyes from reading private data as it is transmitted from server to server and between server and browser. The second benefit, possibly even more important, is establishing that a specific server and domain can be trusted. An SSL certificate can authenticate that a specific server and domain do belong to the person or organisation that it claims to represent. This benefit requires that the hosting provider use SSL from a third-party certificate authority (CA).

SEGREGATING DATA AND SECURING ACCESS TO CLOUD SERVICES

Data segregation risks are ever present in cloud storage. With traditional onsite storage, the business owner controls both exactly where the data is located and exactly who can access it. In a cloud environment, that scenario is fundamentally changed: the cloud service provider controls where the servers and the data are located. However, a proper implementation of SSL can secure sensitive data as it is being transmitted from place to place in the cloud and between cloud provider servers and end users on browsers.

Encryption
Businesses should require their cloud provider to use a combination of SSL and servers that support, at minimum, 128-bit session encryption (or, preferably, the stronger 256-bit encryption). This way their data is secured with industry-standard levels of encryption or better as it moves between servers or between server and browser, preventing unauthorised interceptors of their data from being able to read it.

Authentication
Businesses also should demand that server ownership be authenticated before one bit of data transfers between servers. Self-signed SSL certificates provide no authentication. Only independent, third-party SSL certificates can legitimately deliver ownership authentication. Requiring a commercially-issued SSL certificate from a third-party certificate authority that has authenticated the server makes it virtually impossible to establish a rogue server that can infiltrate the cloud provider's environment.

Certificate validity
Once a server and domain are authenticated, the SSL certificate issued to that device will be valid for a defined length of time. In the rare case that an SSL certificate has been compromised in some way, there is a fail-safe check to verify that the certificate has not been revoked in the time since it was originally issued. Every time an SSL session handshake is initiated, the SSL certificate is checked against a current database of revoked certificates.

There are currently two standards used for this validity check, Online Certificates Status Protocol (OCSP) and Certificate Revocation List (CRL). With OCSP a query is sent to the certificate authority asking if this certificate has been revoked; the certificate authority answers yes or no. If the answer is no, the handshake may commence. CRL, on the other hand, requires that the browser download the most current revocation list from the certificate authority and check the list itself to see if the certificate appears in the list.

The Online Certificate Status Profile (OCSP) standard is considered the more reliable method by many because it is always up-to-date and less likely to time-out due to network traffic. SSL certificates that rely only on the CRL standard are less desirable because in instances of high amounts of network traffic, this step can be missed: some browsers will misinterpret an incomplete CRL review as a confirmation that a certificate is not on the revoked list, consequently completing a handshake and initiating a session based on a revoked SSL certificate. In such a scenario, a rogue server could use a revoked certificate to successfully pass itself off as a legitimate server, creating a ripe condition for a data breach.

HOW DOES SSL WORK?

An SSL certificate contains a public and private key pair as well as verified identification information. When a browser (or client) points to a secured domain, the server shares its public key (via the SSL certificate) with the client to establish an encryption method and a unique encryption key for the session. The client confirms that it recognises and trusts the issuer of the SSL certificate. This process, based on a sophisticated backend architecture laced with checks and double- checks for security, is known as the 'SSL handshake' and it can begin a secure session that protects data privacy and integrity.

FACILITATING REGULATORY COMPLIANCE EFFORTS

Next are the regulatory compliance risks. When it comes to secure and confidential data, businesses are burdened with a slew of regulations. These range from laws like the Sarbanes-Oxley (SOX) Act which affects only public companies, to the Payment Card Industry Security Standard (PCI-DSS), which affects any company accepting payment cards, to the federal Health Insurance Portability and Accountability Act (HIPAA) which affects any businesses with even the remotest possibility of touching patient data. In Europe there is the EU Data Protection Directive (95/46/EC) and Canada has an equivalent Personal Information Protection and electronic Documents Act (PIPEDA).

When an organisation outsources IT to a cloud service provider, the organisation is still responsible for maintaining compliance with SOX, PCI, HIPAA and any other applicable regulations – and possibly more depending on where the servers and the data are at any given moment. As a result, the enterprise will be held liable for data security and integrity even if it is outsourced. Since the enterprise IT manager cannot rely solely on the cloud provider to meet these requirements, the enterprise must require the cloud provider to seek some compliance oversight. Cloud computing providers who refuse to undergo external audits and security certifications are 'signalling that customers can only use them for the most trivial functions', according to Gartner.

Additionally, technological changes to the cloud computing environment can unknowingly whittle away at the compliance of a cloud computing provider's customer. Feature upgrades such as permission modifications, new capabilities, introduction of mobile devices and network changes also can affect compliance.[3] Here, as with data segregation, SSL encryption thwarts accidental disclosure of protected or private data as regulatory due diligence and data access is automated. SSL encryption renders all sensitive data useless to any third party intercepting or viewing it.

MONITORING DATA PROVENANCE

SSL addresses the third area of risk, data location, in the same manner. Public clouds are like black boxes: while they enable ubiquitous access to data, they also obfuscate the physical location of the servers and the data. But if a cloud provider uses SSL to encrypt data as it changes places, an enterprise can be assured that its data will be secure as it moves around the cloud.

In addition, legitimate third-party SSL providers such as VeriSign Authentication, now from Symantec, will not issue an SSL certificate to a server in an interdicted country such as North Korea and Iran. So, as long as the cloud provider requires trusted authentication and encryption on all their servers through SSL from a certificate authority following such a practice, an enterprise will know that the cloud provider isn't storing their data on IT hardware in these countries.

3. 'Domain 10: Guidance for Application Security V2.1', Cloud Security Alliance, July 2010.

OTHER AREAS WHERE SSL CAN HELP

The enterprise needs to know how their cloud provider, with servers around the globe, safeguards data in the case of a disaster. Gartner states that 'any offering that does not replicate the data and application infrastructure across multiple sites is vulnerable to total failure', and that any business in the cloud has a duty to know if the cloud provider is able to completely restore data from backups or duplicates and how long it will take. To prevent data loss, cloud service providers should maintain backup data repositories. If a crash happens, cloud hosts will attempt to recover data from backup servers. SSL adds an extra layer of protection to the backup and recovery process for a business, ensuring that data accessed from backup or duplicate servers is encrypted in transit and that servers being accessed for backup data are authenticated as legitimate sources for that information.

USING SSL CERTIFICATES TO ESTABLISH TRUST IN THE CLOUD

Using a cloud service provider requires a high level of trust and confidence. Business critical applications cannot rely on trial and error. Businesses must insist upon a critical reliability equation to establish trust and SSL certificates provide a highly visible and immediately recognisable way to accomplish that. Alternately, missing or broken SSL can destroy trust instantly.

For example: suppose an enterprise chooses a cloud provider to host their e-commerce website, but the host has a problem with the site's SSL certificate. A user visits the site and is immediately greeted with the alarming 'Secure Connection Failed' error or 'There is a problem with this website's security certificate' message. Will that user ignore the browser warning and click through to complete a transaction on a seemingly-untrustworthy site? Not likely.

The chain of trust extends beyond the cloud vendor to their security provider. The cloud vendor's security is only as good as the reliability of the security technology they use. Cloud providers should be using SSL from an established, reliable and secure independent certificate authority. Its SSL should deliver at minimum 128-bit session encryption and optimally 256-bit encryption. And it should require a rigorous authentication process.

Additionally, some providers may use servers with Debian-based operating systems to generate their SSL keys. The fundamental encryption capabilities of this system were compromised from 2006 to 2008. Enterprises should make sure their cloud provider is not relying on servers nor SSL certificates which may be have been compromised by this flaw. SSL certificates can be issued for validity lengths of up to six years, so it is possible that SSL with this flaw is still being used.[4]

Authentication generates trust in credentials

Trust of a credential depends on confidence in the credential issuer, because the issuer vouches for the credential's authenticity. Certificate authorities use a variety of authentication methods to verify information provided by organisations.

NOT ALL SSL CERTIFICATES ARE CREATED EQUAL

Enterprises need to make sure their cloud provider uses an SSL certificate that cannot be hacked. Make sure your cloud hosting provider can meet these requirements:

- *A Certificate Authority that safeguards its global roots behind layers of industrial-strength security, employing multiple levels of electronic and physical security measures.*
- *A Certificate Authority that maintains a disaster recovery backup for its global roots*
- *Global roots using the strong new encryption standard employing 2048-bit RSA keys.*
- *A chained hierarchy supporting their SSL certificates. At least one intermediate root in the chain adds an exponential level of encryption protection to prevent attacks to the global root.*
- *Secure hashing using SHA-1 or SHA-2 hash algorithm to ensure that the content of certificates can not be tampered with.*

4. Source: http://voices.washingtonpost.com/securityfix/2008/05/debian_and_ubuntu_users_fix_yo.html

It is best to choose a cloud provider who standardises on a certificate authority that is well known and trusted by browser vendors, while maintaining a rigorous authentication methodology and a highly reliable infrastructure. There are four levels of authentication for SSL. All enable an encrypted exchange of information; the difference lies within the strength of the server and domain authentication – in other words, the amount of effort put into validating the ownership and control of that server and domain.

1. **Self-signed certificates** offer zero authentication to enable encryption, and that is all. This type of SSL does not provide the security required by an enterprise.
2. **Domain validated certificates** offer only basic authentication because they only confirm that the person applying for the certificate has the right to use a specific domain name. These certificates are not recommended for server-to-browser connections because they do not vet or display the identity of the organisation responsible for that domain or server.
3. **Organisation validated certificates** offer reliable authentication for the cloud because they validate that the organisation claimed to be responsible for the domain or server actually exists and that the person applying for the SSL certificate for that domain or server is an authenticated representative from that organisation. These SSL certificates are acceptable choices for server-to-browser connections, but they do not offer the highest level of confidence-building features for the end user.
4. **Extended validation certificates (EV)** are the best choice for server-to-browser connections because they offer the strongest level of authentication and the clearest validation that the connection is secure. With EV certificates, the legal, physical and operational existence of the organisation is verified, as is the right of that organisation to use that domain. Using EV ensures that the organisation's identity has been verified through official records maintained by an authorised third party and that the person requesting the certificate is an authorised agent of the organisation.

An SSL certificate with this highest level of authentication can uniquely trigger unmistakable identifiers in an end user's web browser: a green browser address bar that displays the name of the organisation and the name of the certificate authority which issued the SSL. When end users encounter the green address bar, they have complete assurance that their connection is secure. Numerous businesses have reported noticeable uplifts in completed transactions (18 per cent on average for VeriSign Authentication customers) after deploying Extended Validation SSL. For these and other reasons, EV is the preferred choice for hosting applications and services in the cloud.

CONCLUSION: GO WITH WHAT YOU KNOW

SSL is a proven technology and a keystone of cloud security. When an enterprise selects a cloud computing provider, the enterprise should consider the security options selected by that cloud provider. Knowing that a cloud provider uses SSL from a trusted certificate authority can go a long way toward establishing confidence in that provider's commitment to safeguarding the data in its possession. When selecting a cloud service provider, enterprises must also be very clear with their cloud partners regarding handling and mitigation of risk factors not addressable by SSL. Enterprises should consider the seven categories suggested by Gartner when evaluating (and contracting with) cloud computing solutions.

Cloud providers should be using SSL from an established, reliable and secure independent certificate authority. Its SSL should deliver at minimum 128-bit encryption and optimally 256-bit encryption based on the new 2048-bit global root. And it should require a rigorous authentication process. The SSL issuing authority should maintain military-grade data centres and disaster recovery sites optimised for data protection and availability. The SSL certificate authority needs its authentication practices audited annually by a trusted third-party auditor. VeriSign® Authentication offer SSL products that meet these requirements.

More information

Visit our website

www.verisign.co.uk

To speak with a product specialist

Call 0800 032 2101 or +44 (0) 208 6000 740

About Symantec

Symantec is a global leader in providing security, storage and systems management solutions to help consumers and organisations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

Symantec World Headquarters

350 Brook Drive, GreenPark
Reading, Berkshire
RG2 6UH, United Kingdom