Smart Card and Client Certificate Authentication for Web-Enabled Applications
Executive Summary

Whether companies are conducting business online or a government is providing e-services to citizens, it is essential that organizations make these transactions secure. The advanced persistent threats of cybercrime and cyberattacks can result in the loss of national intelligence, intellectual property, and personal information. To combat these threats, companies must find ways to effectively manage and secure the sharing of sensitive information across citizens, public servants, employees, contractors, vendors, government agencies and other organizations.

The vast majority of public and private sector organizations around the world rely on technologies based on Public Key Infrastructure (PKI). PKI-based technology, such as those based on the Transport Layer Security (TLS), can effectively secure information online. However, these technologies underscore significant challenges related to application scalability and performance, especially for organizations serving large audiences and operating under diminishing infrastructure budgets.

This white paper describes how Akamai’s distributed platform is uniquely positioned to help organizations around the globe overcome the challenges associated with PKI-based solutions, allowing them to focus on best serving citizens, partners and customers.

How Akamai Delivers a Better Internet

The Akamai Intelligent Platform™ is the world’s largest globally distributed content and application delivery platform. It is a network of more than 200,000 servers in over 100 countries around the globe. Servers are co-located with Internet Service Providers (ISPs), enabling Akamai to sit at the edge of the cloud close to end users. At its core, the Akamai platform relies on applied mathematics and algorithms to help solve congestion and availability problems on the Internet.

Anyone using the Internet for anything – to enroll in a healthcare plan, apply for a passport, download music or software, check the headlines or book a flight – is probably benefitting from Akamai services without even knowing it. Akamai plays a critical role in getting content from providers to consumers. As a digital operating environment for the web, the global Akamai platform helps the Internet withstand the crush of daily requests for rich, dynamic and interactive content, transactions and applications. When delivering on these requests, Akamai detects and avoids Internet problem spots and vulnerabilities, enabling websites to perform optimally, media and software to download flawlessly and applications to perform reliably.

By taking advantage of Akamai’s managed services on top of this platform, hundreds of enterprises as well as governments worldwide sell, inform, entertain, advertise, deliver software and conduct mission-critical business online. Organizations can be up and running and delivering their websites and applications via the platform in a few days or less. Once organizations are using Akamai’s services, they gain insight into worldwide Internet conditions and access to tools to manage their online business through Akamai’s Luna Control Center.

Today, Akamai handles tens of billions of daily web interactions for companies like Audi, NBC and Best Buy, and organizations like the U.S. Department of Defense and NASDAQ – powering brand-new business models that serve changing online mission needs.
What is PKI?

Public Key Infrastructure (PKI) enables users and computers on unsecure public networks, such as the Internet, to share information securely by using public and private cryptographic key pairs. These keys are typically obtained from a trusted authority called a Certificate Authority (CA). PKI leverages electronic documents called digital certificates to bind public keys with identities, such as a person's name, company, address, etc. PKI has been widely adopted across industries as it enables the following in applications:

- **Authentication**: Online systems, such as web portals, can validate the identity of an end user before allowing access to the system.

- **Confidentiality**: Information can be encrypted at rest or in motion, and PKI helps prevent interception by an unauthorized party.

- **Integrity**: Content authors can digitally sign data, providing a high degree of assurance that it has not been modified by an unauthorized party.

- **Non-Repudiation**: Prevents users from claiming (repudiating) that they were not party to a transaction.

The primary function of any PKI is to allow the distribution and use of cryptographic keys and certificates with security and integrity, which provides the foundation for web security services like TLS to operate.

Why Traditional PKI Solutions Fall Short

E-commerce, banking, and financial websites rely heavily on the TLS protocol to secure the transmission of sensitive data – such as credit card numbers and other personally identifiable information (PII) – from customer web browsers to their web servers. As mentioned above, TLS has proven to be effective for securing data transmission; however, it is resource-intensive and consumes a significant amount of web server CPU. About 70% of total processing time for an HTTPS request is spent on TLS processing, which is mainly due to cryptographic operations performed during the transaction. When considering the overhead added by TLS in terms of increased resource utilization and transaction times, online systems must be sized appropriately or performance and user experience will suffer.

This is particularly important when preparing for peak traffic, such as open enrollment or tax season. In order to handle the expected traffic surge, website owners could spend hundreds of thousands of dollars to build out redundant web infrastructure. This includes web servers, application servers, database servers, load balancers, etc. However, when the busy season ends, the large capital expenditure may sit idle because of lower traffic levels during the remainder of the year.

On the contrary, a business or government agency choosing not to invest in additional infrastructure to handle peak traffic is also assuming a significant risk. Just one hour of downtime due to overwhelming traffic levels can be a source of major embarrassment for the organization and erode consumer and citizen confidence.

So which approach is best? Should organizations take the do-it-yourself approach and build out infrastructure? Or do nothing and hope the current infrastructure holds up under peak volume? The answer is: Neither. The optimal solution is to leverage a secure distributed platform like Akamai's, which scales on demand to offload TLS overhead, bandwidth and requests from origin web infrastructure. Such an approach allows commercial entities and government agencies to focus on what they know best: providing customers and citizens with the information, products and services they demand.
Akamai’s PKI-Based Services in the Cloud

Akamai provides a range of PKI-based cloud security services to government organizations and business around the world.

Secure (TLS) Website Delivery

Delivering secure, TLS-protected sites and high performance at high loads often requires organizations to overprovision their infrastructure due to the CPU and bandwidth intensive nature of TLS interactions. Akamai relieves content providers of this burden by offering significant scalability without sacrificing performance or reliability.

TLS sites are delivered over a specially designed, dedicated portion of the Akamai global network. The Akamai Secure Content Delivery Network has been designed by Akamai’s web security experts from the ground up to meet the highest levels of physical, network, software and procedural security. Akamai’s servers are placed in data centers featuring high levels of network security, in locked cabinets monitored by cameras and other devices to detect unauthorized access. Proprietary Akamai software deployed on these servers safeguards private and sensitive information. Moreover, Akamai’s servers are continuously monitored and audited for integrity. Documented procedures govern the access, updates and maintenance of all servers and software. Only a select number of highly trained and authorized personnel are allowed to access and modify these systems.

To enable Akamai to serve a customer’s secure content, Akamai provisions a digital certificate on its Secure Content Delivery platform. Using this certificate, a client is able to establish a secure session with an Akamai Edge Server and access content from the authenticated site. Akamai purchases industry-standard X.509 digital certificates from leading certificate authorities including Symantec, Comodo and Verizon. In addition, Akamai maintains a subordinate certificate authority that allows us to create and issue certificates for Akamai customers. Alternatively, Akamai can support certificates signed by other certificate authorities. In such cases, Akamai generates the private key and provides the Certificate Signing Request (CSR) to the customer. The customer must then have the CSR signed by its chosen certificate authority before returning the signed certificate to Akamai.

Types of Akamai certificates:

- **Extended Validation (EV) Digital Certificate:** A special type of X.509 digital certificate that requires more extensive investigation of the requesting entity by the certificate authority before being issued. EV digital certificates may be issued as single-hostname or Subject Alternative Name (SAN) certificates.

- **Standard or Single-Hostname Digital Certificate:** An X.509 digital certificate identifying a single hostname that is issued by either Akamai or an Akamai-chosen certificate authority.

- **Subject Alternative Name (SAN) Digital Certificate:** An X.509 digital certificate standard that can be used to identify more than one entity or device. Digital certificate products identified as SAN digital certificates can sign more than one hostname.

- **Wildcard Digital Certificate:** An X.509 digital certificate that signs multiple hostnames within a specified domain. For example, the wildcard *.example.com specifies the domain “example.com” and can sign hostnames such as “www.example.com” and “images.example.com”. Wildcard digital certificates are issued by either Akamai or an Akamai-chosen certificate authority.
Below is a diagram depicting secure (TLS) website delivery over Akamai’s distributed computing platform.

1. Akamai’s dynamic mapping system routes end-user requests for secure application content to the optimal Akamai edge server. A TLS connection is established between the end user and the Akamai edge server.

2. Route optimization technology identifies the fastest and most reliable path back to the origin infrastructure for the retrieval of dynamic application content.

3. Several connection techniques are used to optimize the TLS connection between the Akamai edge server and the origin infrastructure, improving the performance and reliability of the content retrieval.

4. The Akamai edge server retrieves the requested application content and returns it to the requesting end user over secure, optimized connections.

X.509 Smart Card and Soft Certificate Validation

X.509 smart cards look and feel like credit cards, however they come with embedded microprocessor chips that can be programmed in different ways. For the purposes of this paper, the term smart card refers to X.509 client certificates that are signed by certificate authorities and used by network clients (e.g., end users) to authenticate to web servers or other online devices. Soft certificates are the virtual equivalent to the X.509 smart card where the certificates are stored on the user’s computer rather than on a physical card.

Client certificates enable organizations to perform two-factor authentication on end users before allowing logical access to enterprise applications. This provides mutually authenticated TLS sessions since the user and web server authenticate each other during the TLS handshake. The end result is a two-way TLS session that is arguably the strongest form of authentication available on the web today. In fact, this is more secure than all forms of username/password authentication that can be performed over standard (one-way) TLS.

Client certificates also enable holders to digitally sign documents and perform legal transactions online. By using client certificates, all parties can be confident in the identity of the party that digitally signs a document (a concept also known as non-repudiation).
Because of the web security benefits associated with client certificates, organizations around the world have issued smart cards to employees, customers, vendors and other parties that touch their business. Some governments even mandate the use of smart cards, such as through United States Homeland Security Presidential Directive 12 (HSPD-12) and national smart card ID programs in many countries. By doing so, they enable secure information sharing online. In each case, the number of X.509 Smart Cards issued to end users may range from tens to hundreds of millions. In fact, many countries around the world now use PKI and digital certificates as a primary means of determining citizen identity and access to services. For instance:

- In Estonia, the national ID card enables citizens to participate in national elections online.
- Belgium has implemented a program known as “eID”, which is a card containing a chip that holds citizens’ personal information, such as address, as well as digital signature keys and certificates.
- Italian municipalities utilize an electronic identity card known as “Carta d’Identità Elettronica” which citizens use for both online and offline identification. This card was designed to give access to e-government services and will become the standard for access to online services offered to Italian citizens by public authorities.

Although Smart Card PKI systems provide an ideal framework for secure data exchange, the technology is resource-intensive and difficult to scale across large global user bases. It is also important to note that the success of HSPD-12 and other similar initiatives will largely depend on the availability and performance of the Smart Card validation infrastructure from the end-user’s perspective. End users will quickly become frustrated with systems that have availability issues or are slow. In fact, these issues will likely hinder the adoption of PKI-related technology such as Smart Card-enabled enterprise applications.

Akamai helps organizations with these challenges by providing globally distributed X.509 client certificate validation services for authenticating end users as they log in to secure websites over HTTPS. During the validation process, Akamai ensures that the X.509 client certificate is valid and signed by one of the customer’s trusted certificate authorities. In addition, the Akamai platform is equipped with a built-in Online Certificate Status Protocol (OCSP) client that can query the certificate authority’s OCSP responder to ensure the client certificate has not been revoked. If the certificate is deemed invalid for any reason (e.g., expired, revoked, etc.), the end user is blocked by the edge server, preventing unwanted hits and bandwidth from impacting the organization’s application.
The following diagram depicts the client certificate validation flow via Akamai:

1. User inserts PKI credentials in the form of an X.509 client certificate and submits an HTTPS request to a URL that is leveraging Akamai’s Secure Content Delivery service.

2. The Akamai platform routes the user to an optimal edge server based on their location on the Internet, network latency and load across the Akamai platform. The user connects to Akamai over HTTPS and Akamai requests the user’s PKI credentials. The user selects a suitable X.509 certificate and the public key is sent to Akamai during the TLS handshake.

3. The Akamai server confirms the certificate is valid and not expired.

4. The Akamai server then performs a revocation check by submitting an OCSP request to the CA’s OCSP responder and then caches the OCSP response for a configurable period of time.

5. If the certificate is deemed valid and not revoked, Akamai will forward the end-user request along with the certificate payload to the origin infrastructure.

6. The origin server authorizes the end user to ensure they’re allowed to access the requested URL.

Client certificate validation, powered by Akamai’s Secure Content Delivery platform, enables customers to take advantage of all the web security benefits that smart cards and soft certificates offer, such as Two-Factor Authentication. At the same time, they benefit from the performance, scalability and reliability benefits that Akamai’s globally distributed network provides.

**Certificate Revocation Checking**

A critical component of any PKI is the certificate validation approach used to ensure certificates are not revoked or suspended. In order to be effective for government agencies, the validation approach must scale to millions of users while providing high performance and high availability in a cost-effective and secure manner. Whether an organization – such as the Department of Defense – runs its own PKI or operates as a commercial certificate authority, the number of certificate revocation checks will grow as the number of issued certificates rises. Since the use of PKI has permeated all industries around the globe, there is now a critical need for highly scalable and reliable revocation checking services such as those enabled by OCSP and Certificate Revocation List (CRL) delivery.

Akamai can increase the performance and scalability of an organization’s OCSP solution, even if that solution uses the OCSP Authority Information Access (AIA) field on the client certificates. This ensures that end users are able to authenticate their sessions no matter how much traffic is being directed at the OCSP servers, even in the event of a denial-of-service (DOS) attack. The following describes how Akamai can enhance the performance and availability of an organization’s OCSP and/or CRL delivery services.
CRL Delivery From the Cloud

If an organization requires email to be digitally signed, then it likely understands the performance and network burden caused by revocation checking via CRL files. CRL files contain a list of certificates (or more specifically, a list of serial numbers for certificates) that have been revoked or are no longer valid and therefore should not be trusted. Email clients like Microsoft Outlook can be configured to download CRL files to perform a revocation check on the email sender’s certificate. Since some organizations’ CRL files are hundreds of MBs in size, their email clients can experience serious performance degradation while also consuming a significant amount of bandwidth.

Akamai can help with the performance, scalability, and bandwidth problems caused by CRL files. First, since CRL files are cacheable web objects, they can be staged in the Akamai Cloud closer to end users. This enables Akamai to deliver CRL files to clients considerably faster when compared to non-distributed (i.e., centralized) web infrastructures. As proof, see the performance results below from a series of performance tests Akamai conducted with a large Federal Government customer. The chart shows that Akamai boosted performance 29x on downloads of a 2 MB CRL file.

In addition to the performance benefits noted during this test, Akamai offloaded 98% of all CRL file requests from the organization’s directory service. By doing so, Akamai enabled the application to seamlessly scale on-demand for the duration of the test. The below graph shows the 98% bandwidth savings the enterprise application experienced during the performance test.

Because Akamai shoulders the bandwidth consumption caused by CRL files, organizations can free up bandwidth for other mission-critical applications that share the same Internet connection.

In the above graph, the blue lines represent the Akamai bandwidth (Mbps) consumption during the test and the green lines represent origin bandwidth consumption. The graph shows very few green lines since only a small amount of the organization’s bandwidth was needed to fulfill the CRL file requests during the test.
Conclusion

Simply relying on TLS to enable secure transactions over the Internet is no longer enough to protect truly sensitive information. Leveraging a PKI solution will enable secure information sharing across employees, customers and vendors when simple passwords are not enough. That being said, although PKI-based solutions provide the strongest form of security online today, they can pose significant challenges in terms of scalability, performance and cost.

Whether enabling hundreds, thousands or millions of end users to securely share their information, it’s critical to call upon a highly reliable and distributed computing infrastructure. Many of the most valuable name brands in the world, both commercial and U.S. Government, rely on the Akamai platform. By breaking away from the do-it-yourself model and allowing Akamai to handle the brunt of these resource-intensive transactions, organizations can focus on what they do best – serving their customers and constituents.

4. Two-factor authentication: a security process in which the user provides two means of identification, one of which is typically a physical token, such as a smart card, and the other of which is typically something memorized, such as a pass code. (http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci992919,00.html)