

Security and The Security of X.509 Certificates

SecureAuth has based its authentication solution on X.509v3 technology (Public/Private Key Infrastructure) for security reasons.

Public/Private Key technology:

1. Validates the authenticity of the User
2. Validates the authenticity of the Server

The second functionality, the authenticity of the server, is a function not possible with other authentication technologies. Technologies such as username/passwords, hard/soft tokens and keystroke and other biometric systems have no mechanism to perform mutual authentication. These systems do not provide any veracity-checking of the server. PKI, however, implements a bi-directional and mutual authentication based on a public/private key on both the user's system and the server.

The cryptographic foundation of X.509 are well established and universally accepted. Every secure web service utilizes certificates to secure transactions. This level of security is not often extended to the end-user due to complexity issues, and SecureAuth's unique value proposition is its secure and user-friendly issuance of the identity certificate.

When the U.S. government felt it needed to address authentication it determined to utilize PKI technology and incorporated private/public key authentication into its HSPD-12 standard. X.509 certificates are utilized to validate both the holders and the server.

Ref: [Homeland Security Presidential Directive \(HSPD\) 12](#)

In addition, all key regulatory guidance recognize PKI as one of the strongest authentication mechanisms, including:

- FFIEC (Federal Financial Institutions Examination Council) regulating all financial transactions in the U.S. Ref: [Authentication in an Internet Banking Environment](#)
- PCI DSS (PCI Data Security Standard for payment brands including American Express, MasterCard, Visa, Discover and others) Ref: [PCI DSS](#) (Section 8.2)

In fact, the chair of a U.S. Federal steering committee, Richard A. Guida, who was tasked on determining a solution for the threats to the internet was quoted as saying:

[Government] agencies confront the issues of user authentication, confidentiality and integrity of data transferred, and the ability to hold transacting parties accountable when necessary. While there are many technologies which meet some of these requirements, only one provides the tools for meeting all of them: public key technology, implemented in the form of a Public Key Infrastructure (PKI).

The National Institute of Standards and Technology in their report titled: "Key Infrastructure (PKI) Technical Specifications: Part A – Technical Concept of Operations p38 (Sept 1998)", stated, in reference to software-based PKI solutions:

Entirely software based solutions are appropriate for many clients and their applications.

(See additional quotes in Appendix A)

Common Misconceptions of “Certificates”

- Certificates are just files that can be e-mailed to other computers and users.

This is an untrue statement, especially in reference to a SecureAuth x.509 certificate. SecureAuth utilizes fingerprinting mechanism to map the certificate key pair to the user and the machine so the certificate and can not be exported.

- Authenticating the computer is *not* a replacement for authenticating the end-user.

The SecureAuth X.509-based solution does not just authenticate the computer. SecureAuth, because it always requires 2-factors, always ask for additional information from the user, such as password before determining the user is valid.

- Also, how is the user authenticated to get new certificates then they go to a new machine? If there's no strong authentication needed to get the certificate, this security method is as strong as its weakest link!

The strength of the SecureAuth solution is that it utilizes out-of-band user-validation technologies such as telephony and SMS to insure that the user is legitimate user, before conducting a X.509 certificate registration.

Summary:

SecureAuth is the superior authentication solution because it uses X.509 public/private key technology to insure the legitimacy of the user. It is through this ease-of-deployment X.509 technology that enterprises are able to conduct a mutual authentication between the end user and the server. Multiple government and regulatory agencies, including the Department of Homeland Security to the National Institute of Standards and Technology (NIST) recognize PKI authentication as not only valid, but the superior user identification system.

SecureAuth utilizes PKI technology for security and then provides additional functionality around the public/private key pair technology for ease of user and enterprise deployment.

Appendix A: Additional PKI government reference

From The Evolving Federal Public Key Infrastructure, p1

While there are many technologies which meet some of these *requirements [user authentication, confidentiality and integrity of data transferred, and the ability to hold transacting parties accountable when necessary]*, only one provides the tools for meeting all of them: public key technology, implemented in the form of a Public Key Infrastructure (PKI).

<http://www.cio.gov/fkippa/documents/pki-brochure.pdf>

From the Public Key Infrastructure (PKI) Technical Specifications: Part A – Technical Concept of Operations, p38

Entirely software based solutions are appropriate for many clients and their applications.

<http://csrc.nist.gov/archive/pki-twg/baseline/pkicon20b.PDF>

From the FPKI CPWG Mapping Comparison Matrix: Citizen & Commerce Certificate Policy (C4) Requirements, p7

2. The identity may be established using procedures similar to those used when applying for consumer credit and authenticated through information in consumer credit databases or government records, such as:

- the ability to place calls from or receive phone calls at a given number;
- or
- the ability to obtain mail sent to a known physical address.

<http://www.cio.gov/fkippa/documents/C4CAmatrix.doc>

FPKIPA Citizen and Commerce Class Common Certificate Policy, V2.1, p9

This policy requires issuance of X.509 version 3 certificates.

http://www.cio.gov/fkippa/documents/citizen_commerce_cp.pdf