Report to

King County

King County

Department of Judicial Administration, Office of the Superior Court Clerk

E-Filing Project

Digital Certificates Recommendation

DRAFT

Sierra
New thinking.

Sierra Systems Group Inc.
10900 N.E. 8th Street, Suite 1110
Bellevue, WA 98004-1455 USA
www.SierraSystems.com

Contact: Shayne Boyd
Phone: 425.586.5316
Fax: 425.451.4430
Email: ShayneBoyd@SierraSystems.com

Date: May 18, 2004

Revision Log: Digital Certificates Recommendation

Revision Date	Description	By Whom
May 11, 2004	Initial document draft	R Morgan

TABLE OF CONTENTS

1. Introduction

1.1. Purpose

The King County Department of Judicial Administration (DJA), Office of the Superior Court Clerk's E-Filing processes enable judicial officers to apply a non-refutable digital signature to court documents. Digital signatures require a secure public and private key pair for signing court documents. Industry best practice uses digital certificates to hold and validate the key pair. This document evaluates potential sources of digital certificates and makes a recommendation for provisioning and using digital certificates for E-Filing judicial officer document signing.

1.2. Background

According to the American Bar Association, written signatures fulfil four functions.

- **Evidence**. The signature authenticates the document by identifying the signer with the signed document.
- **Ceremony**. The act of signing a document draws attention to the legal significance of the signer's act.
- **Approval**. In certain legal contexts, the act of signing expresses the approval or authorization of the document.
- **Efficiency**. A signature on a document imparts a sense of clarity or finality to the document and often lessens the need for subsequent inquiry.

Like their historical counterparts, digital signatures are marks made (electronically) to or associated with a document. To fulfill the historical functions of a signature, a digital signature must have these attributes:

- The signature must indicate who signed the document and must be difficult for another person or persons to reproduce without authorization.
- The signature must identify what is signed, making it impractical to alter or falsify the original document.

To achieve these requirements, most digital signature implementations use a public key infrastructure or PKI mechanism for identifying the individual who signed a document. PKI implementations use digital certificates for identifying the signer providing appropriate levels of security.

The King County DJA E-Filing project has a requirement for a PKI mechanism for judicial officers to sign documents.

2. Comparison of Digital Signature Options

This section describes how digital signatures work and compares the features and providers of digital signatures.

2.1. Overview of Digital Signatures

A digital signature is information appended to or associated with an electronic document used to identify the signer of the document and to ensure the document has not been altered since the signing. The information contained in a digital signature is encrypted to ensure is authenticity and to make it very difficult to forge.

The encryption process is accomplished using a pair of keys—a public key provided to anyone why wishes to send encrypted information to the owner of the key pair, and a private key used to decrypt the information. The process of generating public and private key pairs, protecting the private key and publishing the public key is commonly known as the Public Key Infrastructure or PKI and is beyond the scope of this document.

The process of creating a digital signature is as follows.

The original document is reduced to a few lines called a message digest using a processed called "hashing." The digest uniquely describes the content of the original document. Any alteration or change to the document alters the digest. Thus, the digest can be used to detect unintended alterations to the document. The digest is encrypted using the signer's private key to prevent it from being altered. A recipient wishing to verify the document was not altered since signing need only recompute the digest of the document, decrypt the digest contained in the signature using the signer's public key and compare the two values. This process proves two essential elements in signing a document:

1. The document has remained unchanged since signing—its digest matches the encrypted digest stored in the key, and

2. The document was signed by the owner of the key pair.

Control and verification of the public and private key pair are essential to the reliability of a digital signature. It is essential to know the identity of the key pair owner and that the key pair has not been compromised—that is, the private key discovered by an unauthorized party. This control and verification is provided using digital certificates.

2.2. Overview of Digital Certificates

A digital certificate provides a means to prove electronically an individual's identity. Digital certificates are used to encrypt information so that only the intended recipient can read it, to identify its holder in electronic transactions, to sign information to provide assurance it was not changed or altered and to verify authenticity of signed information.

A digital certificate is issued by a trusted provider ("Provider") who will vouch for the identity of the certificate holder. Digital certificates contain information about the owner's identity and contain the owner's public and private key pairs. The Provider encrypts the certificate using the Provider's private key. Users of the certificate decrypt the certificate using the Provider's public key to (1) verify the identity of the provider and (2) ensure the certificate is unaltered since its creation. The private key contained in a certificate us encrypted using a pass phrase known only to the owner of the certificate. Thus, anyone can use a certificate's public to send private information to the certificate owner, who knows the private key pass phrase. The certificate owner may use the private key to encrypt data such as the signatures digest to verify the signer—the owner of the key, and to verify the information has not been altered.

In general, certificates are issued to individuals and to servers. Server certificates are used to authenticate the identity of a server and encrypt the transmission of data. Personal certificates are used to authenticate the identity of an individual and are used to digitally sign and encrypt electronic documents. To be useful, personal certificates must be available to sign and verify a document. Certificate storage options are

- Stored on a computer hard drive ("standard certificates")
- Stored on a web service provided by the certificate provider ("roaming certificates")
- Stored on a smart card or USB token.

Digital certificates will be issued to judicial officers for the purpose of signing King County DJA E-Filing documents.

2.3. Digital Certificate Providers

Certificate Provider	Certificate Types	Duration	Costs	
			Initial	Renewal
Transact Washington *A secure PKI managed by Digital Signature Trust, DST*	Standard	1 year	$10.00	$10.00
	Roaming	1 year	10.00	10.00
	Intermediate – USB	1 year	80.00	25.00
	Intermediate – Smartcard	1 year	121.00	25.00
	High– USB	1 year	90.00	35.00
	High – Smartcard	1 year	131.00	35.00
	Certificate Coordinator	1 year	250.00	0.00
Thawte	Standard	1 year	0.00	0.00
VeriSign	Standard	1 year	$14.95	$14.95
KC DJA Root CA - *Create King County DJA Certificate Provider*	Standard	n/a	n/a	n/a

Certificate Provider Advantages/Disadvantages

Advantages	Disadvantages
Transact Washington/Digital Signature Trust	
• Recognized by State of Washington • May be AOC default • Several certificate storage options. • Multiple factor identity management • Optional "Certificate Coordinator" program may be used to delegate judicial officer certificate management to DJA or Superior Courts	
Thawte	
• Low cost ($ 0.00)	• Limited certificate options • Single factor identity vetting (SSN, Passport number) • Uses trusted notaries ("web of trust") for identity management
VeriSign	
•	• Limited certificate options • Single factor identity vetting (SSN, Passport number)
King County DJA Certificate Authority	
• Flexible • Low initial cost • Uses existing .NET tools	• May not be recognized or approved by AOC • Requires installation of KCDJA root authority certificate on all county computer systems • Long term costs of deployment uncertain but likely high. May require one or more FTEs to administer.

2.4. Certificate storage

Advantages	Disadvantages
Standard	
• Most common form of personal certificate • Readily accessible and available for signing and cryptographic applications. • Easily managed by most common desktop operating systems: Windows 2000/XP, Macintosh OSx, Linux.	• Certificate must be loaded on each computer used by the certificate owner.
Roaming	
• Certificate stored in secured repository maintained by provider • Certificate is accessible anywhere • Certificate is not installed on hard drive where it may be stolen or copied • Readily accessible and available for signing and cryptographic applications.	• Requires installation of ActiveX control to on client computer to use. • Requires network connectivity and access to the Internet • Only available for Windows and Internet Explorer 5.x, 6.0 and Netscape 4.7x
SmartCard	
• Certificate securely stored on a SmartCard. • Certificate is not installed on hard drive where it may be stolen or copied • Readily accessible and available for signing and cryptographic applications.	• Requires SmartCard reader to be used.
USB Key	
• Certificate securely stored on a USB device. • Certificate is not installed on hard drive where it may be stolen or copied • Readily accessible and available for signing and cryptographic	• Requires USB device and USB port to be used

3. RECOMMENDATION

3.1. Digital Certificates

Sierra Systems recommends King County Department of Judicial Administration, Office of the Superior Court adopt standard Transact Washington digital certificates for judicial officer document signing needs. We make this recommendation for these reasons:

- The Transact Washington digital certificate imposes stronger, multiple factor identification requirements than the other vendors.
- The Transact Washington digital certificate is provisioned and managed by the Digital Signature Trust (DST), the world-wide leader in PKI.
- The Transact Washington digital certificate is fully compatible with the most common desktop applications and operating systems.
- The Transact Washington digital certificate may be required by the State of Washington Administrative Office of the Courts for future PKI applications.

The Sierra Systems recommendation is to use standard, or browser based, digital certificates. We believe this will be most convenient form for King County judicial officers. However, the roaming, USB key and SmartCard certificate options may be evaluated by King County DJA during the pilot deployment of E-Filing digital signing.

3.2. Impact to E-Filing Software Architecture

The changes to the proposed Iteration 2 E-Filing architecture:

- Acquire Transact Washington Digital certificates for judicial officers
- Remove the Valicert (Now Tumbleweed) product as a Validation Authority is no longer required