



X-DSS White Paper

Version 2.03

Public

October, 2008



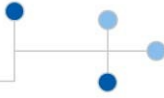
Address

Tel.

Fax

www

Itämerenkatu 5 A FIN-00180 Helsinki +358 9 5860 760 +358 9 5860 7660 www.avaintec.com



Ensuring the Non-Repudiation of Digital Data

Paperless information flows are becoming increasingly common in business, government, and healthcare. They have great potential for reducing logistical costs and increasing productivity through enabling better and faster availability of information while simultaneously protecting it from unauthorized access.

1. Vulnerability To Modification

Digital information is, however, vulnerable to undetectable malicious modification. Anyone with system administrator level access to a computer system can potentially change any information in the system without the possibility of the original information ever being recovered or anyone even knowing that such a tampering has taken place. Such risks can be greatly reduced by taking information security into consideration while designing systems. This can be difficult and expensive, and at its best it relies on “notary” databases, physically protected networks, and similar safeguards. These imprison the information within the system. There still is no way to tell just by looking at the information whether or not it has been maliciously modified, and any verification procedures are logistically heavy and provide, at best, only circumstantial evidence.

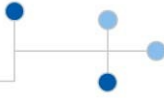
1.1. Ambiguous Legal Status

As a consequence, the legal status of digital information is somewhat ambiguous. While contractual relationships can be and are entered into over digital media, even over insecure networks such as the Internet, the ghost of repudiation always hovers in the background. If a party to a contract stored in digital form claims that the terms have been altered, the situation can be difficult to resolve. Consequently, most important contracts are still printed on paper and signed in the conventional way. This means that much of the productivity potential of digitised information processes is lost or never realized: the end product is still paper that must be physically stored, moved, and copied.

Methods for digitally signing digital documents are clearly needed. These methods must ensure that the information is not altered after it has been signed (integrity) and make it possible to verify which entity produced the signature (non-repudiation).

2. Public Key Cryptography and Signature Standards

The key to the solution was the widespread adoption of Public Key Infrastructure (PKI) cryptography. A trusted third party (governmental entity, bank, or other similar institution), known as the Certificate Authority (CA), issues a digital certificate to an entity whose identity it has verified. This certificate can then be combined mathematically with a representation of the



data to be signed to create a digital signature. Any alteration of the data would break the signature, as any alteration of the certificate would break the certificate. The identity of the signatory can always be verified by requesting information about the owner of the certificate in question from the Certificate Authority while the integrity of the data can be verified by mathematically comparing it with the signature and certificate.

2.1. XML and PKI: A Happy Marriage

The emergence of XML as a semantically rich way of representing digital information has made it possible to use PKI signatures in a wide range of applications. Supporting standards such as Canonical XML (a way of representing XML documents in the unambiguous way required by digital signatures) and XMLDSIG (an XML representation of a digital signature) can make signatures and documents fully portable between information systems. A signed XML document can be transferred from one system to another, and the signatures can be verified at any time by any of the systems, irrespective of its internal information security status. Such a signed digital document is a close analogy to the signed paper document: its integrity and non-repudiability can be independently verified anywhere, regardless of what has happened to the document. In fact, the security of a digital signature greatly exceeds that of a paper signature. Forging digital signatures requires extensive expertise and computer resources, and is in most cases practically impossible.

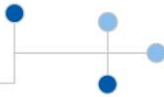
2.2. Digital Signature Legislation

The emergence of technical solutions to the problem of electronically signing digital data has resulted in corresponding changes in legislation. The EU's Directive on a Community framework for electronic signatures (1999/93/EC) ("the Directive") promotes electronic transactions within the EU by establishing certain level standards for the recognition of electronic signatures throughout the Member States. The Directive has been implemented nationally and digital signatures have gained complete legal equality with paper signatures. Any contract, petition, or other document can now be signed digitally.

2.3. Server-Side Signatures and Time Stamps

PKI signatures do not necessarily have to be created by people. In some cases, system signatures are a better solution – the information systems stamps the incoming information as it is received. This provides proof that the information existed in a specific form, although it does not (necessarily) provide information on the human originator of the information.

A particularly important type of system signature is the timestamp: an authority guaranteeing its timestamps to be accurate to within a certain time frame signs representations of incoming information along with the time. This provides proof that the information existed in a specific form at a certain time.



2.4. Downsides of PKI Cryptography

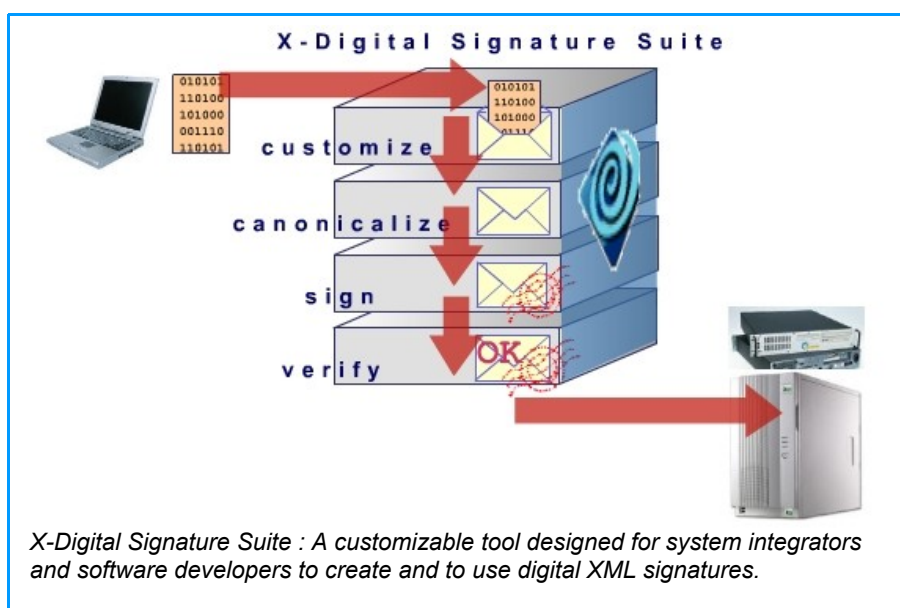
However, PKI cryptography has its downsides. The process for issuing certificates is cumbersome, and requires a heavy infrastructure. Often the certificates reside on smart cards, which require card readers and specialized software on the client applications. Furthermore, most solutions implementing PKI signatures are highly proprietary: the data is stored in closed formats, and can only be verified within the originating system. It cannot be verified independently, and heavy client-side software components are needed to access and to use the data.

Therefore other methods for creating digital equivalents for paper signatures have emerged. These include developments like the Finnish TUPAS bank signature, based on an exchange of key codes between the user and the bank at the time of signing. Some recent developments promise the best of both worlds – the full security of PKI signatures without the client-side complications. E.g. by storing the certificate on the smart card of a cellular phone, the user can sign documents using his telephone.

All of these methods have acquired the legal status of a recognized signature: they are equivalent to the signed paper contract.

Another complication hindering the adoption of digital signatures is that while the principles are fairly simple, digital signatures and other non-repudiation technologies have certain complexities concerning the technology. Implementing digital signatures from scratch would require a significant amount of research and highly specialised skills from the system integrator or software developer.

3. A Packaged Solution for Non-Repudiation Technologies





Avaintec's X-Digital Signature Suite (X-DSS) provides digital signature and non-repudiation technologies in a package that is as simple as possible to integrate into host applications as. It makes it possible to enjoy the full benefits of PKI signatures and other non-repudiation technologies without the requirement of specialized domain knowledge. Any digital data that can be represented as XML (even by simply Base64 encoding it and adding a wrapper element) can be digitally signed with verifiable signatures.

3.1. X-DSS Features

X-Digital Signature Suite provides the following non-repudiation technologies:

1. PKI signature in World Wide Web Consortium's (W3C) standard XMLDSIG format, using smart cards, soft certificates, USB tokens, or other on-workstation certificate.
2. System signing: standard PKI signatures created server-side, using a certificate issued to the server.
3. Time stamping: providing proof that the data existed in a specific form at a certain time by signing it with a system certificate.
4. Signature validation: verifying the integrity of signed data and the status of the certificate used to sign it, including checking revocation lists, time span, and certificate signature.
5. PKI signatures using certificates stored on cellular phones.
6. TUPAS Bank Signatures: ensuring the non-repudiation and integrity of data by exchanging numerical keys with a bank at the time of signature.

X-Digital Signature Suite consists of server- and client-side components. The client-side components consist of a browser plug-in (Microsoft Windows and Linux, Netscape 6.0 and later, Microsoft Internet Explorer 5.0 and later) and a



Javascript library used to access it. The plug-in can be set to auto-install, or it can be installed centrally over a corporate intranet. The server-side components are written as Java Servlets, and are therefore highly portable between different platforms.

It is possible to integrate these components directly into the host application's WWW interface, or alternatively to use a pre-fabricated HTTP Post interface for creating the signatures.

Signature validation has a similar client-side interface: validation functionality can be integrated directly into the user interface, or accessed via HTTP Post. Alternatively, server-side applications can interface with the validation components directly, using the provided Java API.

X-DSS System Signer and X-DSS Time Stamper have standard Java interfaces with which signatures and time stamps can be requested.

3.2. Integrating with X-DSS

At its easiest, adding a digital signature to an existing information system consists of wrapping the data as XML, posting it to an X-DSS interface with an HTTP query, and retrieving the signature from the return message. Validation is likewise easy: simply posting the data and signatures to an X-DSS validation interface with an HTTP query, and retrieving the result from the return message. The X-DSS Javascript API is capable of triggering scripts from the host application when the return message is loaded, further simplifying integration.

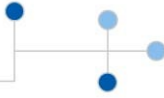
X-DSS can, however, be integrated with its host application at any depth desired. The Javascript libraries and browser plug-in can be imported directly into the host application's WWW interface. In this case, the host application instantiates the objects in X-DSS API and calls its methods directly. A completely seamless user experience can be created by adding a dozen lines of code to the host application.

X-DSS can be integrated into a Microsoft Windows application with a standalone (non-WWW) interface by accessing the API through Microsoft Internet Explorer called through the ActiveX interface.

Server-side, the X-DSS components (in particular, the System Signer, Validator, and Time Stamper) can be accessed via RMI, the standard time stamping interface, or provided Java interface classes. This way, the host application gains the full complementary benefit of signature functionality without having to worry about trivial issues like canonicalisation of data.

4. Technology and standards

- **X-Digital Signature Suite Client:**
 - Operating Systems supported and tested
 - Windows NT, version 4.0 and later
 - Windows 95, SP 1 and later
 - Windows98
 - Windows 2000



- Windows XP
- **Browsers**
 - Microsoft Internet Explorer, version 5.0 and later
 - Netscape, version 6.0 and later
- **Server:**
 - Operating Systems
 - Solaris, version 8.0
 - Linux
 - SuSE 7.2 and later
 - RedHat 7.1 and later
 - Debian 3.0 and later
 - Windows NT, version 4.0 and later
 - Windows 2000
 - Windows XP (only with MS SQL Server 7.0 and later)
 - Java 2 SDK 1.4.x (included as part of installation)
 - Jetty 4.2.x (Included as part of installation)
 - Cocoon 2.1.x (Included as part of installation)

Supported standards:

- XML 1.0
- W3C XML Digital Signature (XMLDSIG) standard
- XML Schema
- Java 2
- HTML 4.01
- JavaScript 1.2
- CSS Level 1
- PKI X.509

5. About Avain Technologies

Avain Technologies develops and tailors user-friendly, networked, secure and flexibly managed ready-made products for companies and organisations, allowing them to implement their service and process flow management and store their information in digital form in the long term. Our solutions enable a phased transition to a fully digital, paperless environment.

Our technology is based on open industry standards, and we participate actively in international standardization forums.

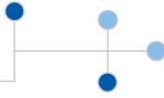
By working in close and interactive cooperation with our customers and partners, we develop products that allow an increasing number of companies and organisations to improve their operations and services, reduce costs and increase the commitment and satisfaction of both personnel and customers.

Our customers include organizations in local and national government, healthcare, and finance sectors.

5.1. Avaintec's values

Our key values are:

- ensuring customer satisfaction,
- respecting the individual in everything and everywhere, and
- offering advanced technology and strive for perfect information security.



5.2. Ownership

Avain Technologies Ltd is owned by its employees and institutional investors, such as The Finnish National Fund for Research and Development (Sitra) <<http://www.sitra.fi/eng/index.asp>>.

5.3. Date of Foundation and Company History

Avain Technologies is a Finnish software company founded in 1997. Its main products are X-Archive, an XML and PKI-based solution for long-term archival of electronic records, X-Web Form Manager, an XML based solution for serving, submitting, signing, and processing electronic forms securely over the Internet, and X-Digital Signature Suite, a component that can be integrated in WWW-based software providing digital signature functionality using PKI, GSM, and other technologies.

5.4. Contact Information

Company:

Avain Technologies Inc.
Itämerenkatu 5 A
FI-00180 Helsinki
Finland

Tel: +358 9 5860 760

Fax +358 9 5860 7660

WWW: <http://www.avaintec.com/>

E-mail: info@avaintec.com