Electronic Filing Technical Standards
For the
Washington State Courts

Authorization

General Court Rule 30 (GR 30), adopted by the Washington State Supreme Court, requires the Judicial Information System Committee (JISC) to adopt electronic court filing technical standards that are to be followed by the courts in the state of Washington that implement electronic filing.

Revision

At the direction of the JISC, the Washington State Administrative Office of the Courts (AOC) shall review the technical standards annually and propose changes to the JISC. The AOC will solicit input from potentially affected courts before submitting its recommendation. The JISC may convene or authorize periodic *ad hoc* working groups to make major revisions as desired.

Business Goals

Electronic filing of court cases is intended to make the business process more efficient and less costly for both litigants and the courts themselves. Technical standards should support and encourage high usage, so that the underlying business case will be realized as soon as possible.

Technical standards support several desirable business goals served by electronic court filing systems:

- **Interoperability**: the ability of a litigant to file electronically in different courts.
- **Flexibility**; the ability to allow litigants to file electronically in courts that use any of several different business models.
- **Openness**: the ability for a court to offer electronic filing so it can be accomplished by multiple electronic filing service vendors.
- **Efficiency**: the ability of any court or filing provider to use standard software for successful electronic court filing.

Strategy

The Washington State Courts seek to use national and industry standards, both *de jure* and *de facto*, whenever possible. At the national level, the Conference of State Court Administrators (COSCA) and the National Association for Court Management (NACM),

Version 0.5
November 7, 2003

working through their Joint Technology Committee (JTC) have endorsed standards for electronic court filing business processes. These standards include some technical standards.

Within the Organization for the Advancement of Structured Information Standards (OASIS), the Legal XML Member Section's "Electronic Court Filing Technical Committee (ECFTC)" has published several proposed standards for electronically filing and querying court systems for data and documents. These standards were developed as Extensible Markup Language (XML) "Document Type Definitions (DTDs)," documents used for standardizing the use of XML in particular areas of application. DTD's themselves are non-compliant with the basic XML standard, so the XML Schema now replaces the DTD as the preferred method for describing documents.

Aside from the problem of using a DTD, the ECFTC standards represent an incomplete technical architecture that leaves many areas of potential interoperability undefined. In particular, the standards do not yet support the correct implementation of web services. They also do not incorporate objects from the latest and most useful version of the national Justice XML Data Dictionary (JXDD), which has been sponsored by and developed under the auspices of the U.S. Department of Justice.

Ideally, state court technical standards would be based on or simply reference the OASIS Legal XML ECFTC standards for electronic court filing. When the ECFTC completes the planned second version of its electronic court filing technical standards, this vision should become realistic. Until that time, the JISC must specify usable technical standards that anticipate the direction of the OASIS ECFTC work.

The JXDD Version 3.0 is still in draft form. Courts and other justice groups are validating the draft with current projects. Version 3.0 represents a breakthrough opportunity to standardize the semantics of justice information in a way that will significantly facilitate sharing justice and public safety data. Court technical standards should reuse the JXDD Version 3.0 XML objects wherever possible.

The Washington State and Georgia Administrative Offices of the Court (AOC's) are jointly sponsoring the Open XML Court Interface (OXCI) project to create a court filing middleware application or Electronic Filing Manager (EFM) that will be compliant with national standards and can be used by any court. It constitutes only part of a complete electronic filing architecture as envisioned by OASIS Legal XML's ECFTC. The JIS Committee plans to offer the OXCI middleware statewide, once it is completed, for Electronic Filing Service Providers (EFSP's) to file directly with the JIS case management system.

The COSCA/NACM and OASIS standards have been written flexibly enough to support a number of different business models for implementing electronic filing. In principle, the technical standards should be indifferent to where the various components of the architecture reside (in the court or with a vendor, locally or remotely). They also can

accommodate a court having multiple electronic filing service providers, some of which may be commercial.

For many areas of functionality, Internet standards from the World Wide Web Consortium (W3C) and OASIS or *de facto* industry standards already exist. Because of their widespread acceptance and success, they should be used. Examples include Hypertext Transport Protocol (HTTP) and HTTP Secure (HTTP/S), Secure Socket Layer (SSL), Transmission Control Protocol/Internet Protocol (TCP/IP), Extensible Markup Language (XML), and XML Schema.

The Washington State AOC believes that software industry is also standardizing on XML Signature & Encryption, Simple Object Access Protocol (SOAP), SOAP with Attachments, Web Services Description Language (WSDL), and Universal Description Discovery and Integration (UDDI) protocol.

Several recently approved security standards likely to become widely implemented are Security Assertion Markup Language (SAML) and Extensible Access Control Markup Language (XACML). Draft standards of possible interest include Web Services Reliable Messaging (WSRM) and Web Services Business Process (WSBP).   A possible alternative to SOAP, WSDL, UDDI and WBRM is Electronic Business XML (ebXML).

Components and Interfaces

The OASIS Legal XML ECFTC intends to create standards that support both interoperability and multiple business models. These potentially inconsistent goals can both be achieved by specifying a flexible component architecture. The components themselves can be visualized as "black boxes," so long as their interfaces and interactions are governed by the open standards. The basic components are:

- Electronic Filing Service (EFS) - provides the interface for actual filing of court documents electronically
- Electronic Filing Manager (EFM) - provides middleware between the electronic filing service and the "back end" case management and document management systems in the court
- Adapters - custom software that connects an EFM with the specific CMS and DMS in the court
- Case Management System (CMS) – a system in which court case data is recorded and in which it is retained
- Document Management System (DMS) – a system that holds the court's case documents and makes them accessible

The OASIS Legal XML ECFTC will define open standards for the following interfaces:

- The Electronic Filing Service (EFS) to/from the Electronic Filing Manager (EFM)
- The Electronic Filing Manager (EFM) to/from the Case Management System (CMS)

- The Electronic Filing Manager EFM to/from the Document Management System (DMS)

Business Models

The OASIS Legal XML ECFTC envisions business models ranging from one extreme, where the court exclusively controls all components of the system, to another extreme where a commercial vendor controls all components on behalf of the court. Variations may include all possible combinations of single vendors, multiple vendors, and courts owning/managing a few, some or almost all of the components. The interface standards for the components are intended to be transparent. That is, they should serve equally well any of these business model variations. The Washington State technical standards will impose some constraints on the allowable business models without eliminating court flexibility or market competition.

Technical Standards

1. Messaging.

   - EFS to EFM and EFM to Adapter messaging shall use SOAP 1.1 (or later) or ebXML 2.0 (or later) messaging standards, bound to HTTP.
   - The initial messaging specification is limited to the SOAP or ebXML messaging standards, with any legal extensions left to the court or vendor.

   COMMENT: The interim messaging specification will be the OXCI messaging schema, for which the estimated availability is March 2004. The final messaging specification will be the OASIS Legal XML Electronic Court Filing 2.0 schema, whose estimated availability is June 2004.

   - Any messages between electronic filing components that travel over any network segment outside the court firewall must use HTTP/S and SSL.

2. Envelope

   - The initial specification for the electronic filing envelope is the OASIS Legal XML Court Filing 1.1 DTD. Minor modifications, extensions and conversion to a schema are all allowable, since this specification was never intended to be a complete specification.

   COMMENT: The interim specification will be the OXCI envelope schema, whose estimated availability is March 2004. The final specification will be the OASIS Legal XML Electronic Court Filing 2.0 schema, whose estimated availability is June 2004.

3. Filing

- An EFS may accept a filing in any file format it chooses to accept and support.
- An EFS must submit a filing to an EFM in one or more of the following formats: TIFF, PDF or standardized XML Schema.
- An EFM must accept TIFF, PDF or XML Schema filings, even if the court converts the filings to one standard format for use and retention in its DMS and/or CMS.
- Courts are free to convert filings from the EFM to their preferred formats for storage in their DMS. The AOC recommends using PDF over TIFF for images in the DMS, PDF for word processed documents in the DMS, XML Schema or PDF with XML (Acrobat Version 6 or higher) for XML-tagged online fillable forms or for XML templates in the DMS.
- XML Schema for XML-based court forms and documents will be released gradually by the AOC. So long as an official state schema does not exist, EFS providers should base the internal tags of their forms and document schemas upon the JXDD Version 3.0 wherever possible.

4. Security

- Litigants or lawyers requesting filing privileges or persons authoring documents to be filed in a court must provide to an EFM (through an EFS) the following identifiers in order to be authenticated for system access: name, date of birth, gender, and driver's license number **or** state identification card number. Requesters will receive an electronic filing system ID, password and Personal Identification Number (PIN). Estimated availability for this identity validation service from AOC to EFS and EFM providers is February 2004. Estimated availability of the Web services specification is January 2004.
- The court or EFM provider is not required to verify any identifying information provided before issuing an ID, password and PIN to a user. Liability for fictitious or incorrect identification information rests with the filer and EFS provider.
- The EFM will log users by identification, time and transaction for the purposes of establishing filing/authoring non-repudiation.
- The EFS must apply a one-way hash to the data/document being filed by an external EFSP to an internal EFM and identify the hash method according to guidance in the technical standards for the purposes of data/document integrity.
- Digital signatures may be required by an EFS to meet its own authentication and integrity requirements, but a court may not require such digital signatures for the purposes of filing authentication.
- An EFM must pass through and preserve any digital signature submitted with a document, but it is not required to use it for the purposes of authentication, non-repudiation, or verification of integrity.
- A judicial officer must use a digital signature with all judicial orders, in order to meet the requirements for non-repudiation and integrity.

5. Policies

- The initial specification for court policy is the Nebraska AOC Court Policy schema.

  COMMENT: The interim specification will be the OXCI Court Policy schema, for which the estimated availability is March 2004. The final specification will be the OASIS Legal XML Electronic Court Filing Policy 2.0 schema, for which the estimated availability is June 2004.

6. Payments

- An EFS provider must collect and transfer required fees and fines to the courts electronically using standard merchant bank mechanisms. This provision applies only to non-court EFSP's.
- An EFS provider must support online payments.
- An EFS provider must provide electronic monthly reconciliation reports to each court for their transactions. This provision applies only to non-court EFSP's.
- The AOC shall provide the technical specification for the reconciliation reports.
- An EFS must indicate the successful receipt of payment in real-time to an EFM before the associated filing transaction may be considered complete.
- The liability for actual payment to the court resides with the EFS provider.
- The EFM must log assertions of payment by the EFS.

7. Components

- A court may use only one official EFM.
- A court may use one or more official EFS providers.
- All courts and vendors operating an EFS and/or an EFM must be certified by the Washington State AOC, which will verify compliance with the technical standards. This process includes execution of a formal contract that also binds the contractor to conform with other legal requirements on related matters, including privacy, data reuse for commercial purposes, and confidentiality. Upon adoption of these standards by the JISC, the AOC will make the certification service and an example contract available.

8. Grandfathering

- Courts operating electronic filing pilot projects prior to formal adoption of these technical standards will be exempt from these technical requirements.
- Initially "grandfathered" courts shall comply with these technical standards in the next major budget cycle after these standards are published.
- Courts shall comply with updated versions of these technical standards in the next major budget cycle after revisions are published.

9. Notice and Service

- Messaging standards for EFS and EFM components shall include requirements in support of standard court noticing and legal service capabilities:
    - notice to filer of filing date and time
    - notice to filer of document problem
    - notice to filer of successful or unsuccessful payment
    - notice to filer of filing acceptance
    - notice to filer of offline system status
    - notice to filer of submitted judicial draft order
    - notice to filer of change in court policy
    - service to case parties
- Filers and EFS providers need not use these capabilities if they prefer direct email communications.

JIS Considerations

For courts using JIS as their CMS, the JIS Committee offers the following issues for their consideration:

- The court will need to specify a version of Court Policy that incorporates state and local rules as well as necessary information about JIS itself. A version of the Nebraska court policy schema using the JIS example may be obtained from the AOC after adoption of these standards.
- The court will also need to specify a standard interface for communication between JIS and the court's DMS. Estimated availability of a published JISC standard by the AOC for a JIS-to-DMS interface based on XML is March 2004.
- The JIS Committee plans to implement special interfaces to JIS for filing of traffic citation and criminal cases. Estimated availability of the traffic citation filing XML schema is January 2004. Estimated availability of the criminal filing XML schema is yet to be determined.
- Courts, vendors and filers will need to know which EFS and EFM providers are certified by the JIS Committee. The AOC will publish information identifying certified providers on the state court web site after adoption of these standards.

Appendix A
Electronic Filing Glossary

These definitions are not normative or part of the official technical standards. They are provided to clarify the intent of the technical standards.

API - Application Program Interface. A formal specification describing how one program can "talk" to another program.

CMS - Case Management System. An application like SCOMIS. A given court's CMS can include non-JIS local systems.

DMS - Document Management System. An application like the King County Superior imaging system, although it would use an XML-based transmission envelope for adding documents into this system.

EFM - Electronic Filing Manager. An application that accepts an XML file from the EFSP application and processes it, passing data to the CMS and DMS, and returning any necessary XML-formatted information to the EFSP application.

EFSP - Electronic Filing Service Providers. EFSP's provide an application for filers to use to submit documents to courts, electronically forwarding those filings to courts, and directing responses from courts back to the respective filers.

HTTPS - HyperText Transfer Protocol Secure. A secure version of the Internet protocol for transmitting information on the World Wide Web. It allows implementation of SSL in servers and browsers, which ensures that information is protected from prying eyes.

PDF - Portable Document Format. An open but proprietary standard for Internet documents from Adobe. PDF preserves the original format of the document. A PDF document that was word processed is text-searchable.

SSL - Secure Sockets Layer. SSL works together with HTTPS to provide encrypted and digitally signed transactions over the Internet.

TIFF - Tagged Image File Format. TIFF is a standard file format for exchanging graphical images.

XML - Extensible Markup Language. XML is an Internet protocol for giving semantic meaning to data elements and document subsections. XML is similar in design to HTML, but XML supports intelligent data exchanges.

Generic Court Filing Business Process

This business process is not normative or part of the official technical standard. It is provided to clarify the intent of the technical standards. It is based on the national functional "process" standard for electronic filing adopted by COSCA and NACM. The national functional standard can be accessed at the web site of the National Center for State Courts.

Access System

1. Litigant accesses web site.
2. System assigns user ID and password.
3. Litigant logs on.

File Case or Document Externally

1. Litigant initiates case.
2. System assigns case number.
3. **[O]** Litigant converts document to acceptable format.
4. Litigant submits filing.
5. **[A]** Litigant submits mass filing.
6. **[A]** Litigant submits draft document.
7. **[A]** Litigant submits non-case file document.
8. System assign unique identifier to document.
9. **[O]** System marks document as confidential.
10. **[O]** Litigant requests confidentiality for document.
11. System notices filer of filing date and time.
12. System checks document for problem (integrity, virus, digital signature, format, etc.).
13. System validates document.
14. **[A]** System rejects document.
15. **[A]** System notices filer of document problem (integrity, virus, signature, format, etc.).
16. System queues document for clerk review.
17. Clerk reviews document.
18. Clerk validates document.
19. **[A]** Clerk rejects document and notices filer.
20. **[O]** Litigant submits filing fee payment.
21. **[O]** System notices litigant of successful payment.
22. **[A]** System notices litigant of unsuccessful payment.
23. System submits document to DMS and dockets CMS.
24. System creates audit log of transaction.
25. **[O]** System creates backup copy of court document.
26. **[O]** System prints paper document.

27. System notices filer of filing acceptance.
28. **[A]** System notices filer of offline status.

File Case or Document Internally

1. Prosecutor initiates case.
2. System assigns case number.
3. Prosecutor submits filing.
4. System assign unique identifier to document.
5. System checks document for problem.
29. System validates document.
30. **[A]** System rejects document.
31. **[A]** System notices prosecutor of document problem (integrity, virus, signature, format, etc.).
6. **[A]** Clerk submits filing.
7. **[A]** Judicial officer approves draft order.
8. **[A]** Judicial officer notices litigant about submitted draft document.
9. **[A]** Judicial officer submits signed court order.
10. **[A]** Clerk files court order.
11. System submits document to DMS and dockets CMS.
12. System creates audit log of transaction.
13. **[O]** System creates backup copy of court document.
14. **[O]** System prints paper document.
15. System notices prosecutor of filing acceptance.
16. **[A]** System notices filer of offline status.

Request Information

1. Litigant requests information (court policy including payment information, case information/data, court document).
2. System returns information (court policy including payment information, case information/data, court document).

Notice and Service

1. Litigant services a case party.
2. System services a case party.
3. **[O]** System notices litigant of change in court policy.

Administer System

1. Clerk maintains access rights.
2. Clerk maintains court policy. **[I added this one. It is not in the King draft.]**

3. Clerk changes confidential status of document.
4. **[O?]** Clerk exports case record to another court.
5. **[O?]** Clerk imports case record into court.

DMS Functions

1. Judicial officer annotates court document.
2. Judicial officer views annotation of court document.

CMS Functions

1. Court user accesses court document in DMS from the CMS.

External Functions

1. Litigants communicate.
2. Clerk converts electronic formats of old court documents.
3. Clerk migrates legacy data to new format.
4. Clerk migrates court documents and data to new DMS and CMS.
5. Clerk responds to disaster.