Accreditation, Certification and Assessment Models

Prepared by Daniel Greenwood, Esq.
Delivered to the EAP EAC Workgroup on June 9, 2004

I. Introduction

This document represents the results of research and evaluation of several accreditation, certification and/or assessment models that provide relevant options for the EAP. This document is in response the Task Order and subsequent refining discussions with and by the EAP EAC Workgroup. The original Task Order is contained in Addenda 1. Addenda 2 includes all previous memos and case studies, to complete the record of original research.

II. Business Goals:

It is useful to reiterate the basic goals of the EAP, as reflected on the EAP web site and the majority of the presentations. The stated goals are to enable interoperability between public and private authentication systems by:

1. Drafting rules for credentials and authentication systems for different and hierarchical assurance levels. These rules should provide a standard set of criteria for evaluating credentials at each assurance levels.

2. Developing a means to (a) assess credentials and systems against the standard set of criteria and (b) convey that assessment to relying parties.

3. Drafting 'rules of engagement' for relying parties that will allow them to use third party credentials. These rules would take the place of bilateral agreements.

4. Creating operating rules for validating credentials and defining how validation of credentials will be conducted.

III. Five Models

1. National/International Accreditation/Testing Regimes

This contains the most detailed and evolved documentation, business models and system of cross-border recognition of all the options investigated to date. While many of the national organizations are governmental or quasi governmental, examples selected for this analysis are all private non-profits (hence, the German DAR has been replaced in this draft by the United Kingdom, and other relevant organizations have been added).

More information on the potential applicability and relevance of this model appears as attachment 1 of addenda 2.

2. Higher Education Accreditation (US Market)

This model was discussed in some detail at the last meeting. In the interests of time, a deeper written description will be deferred until the submission for the next draft so that the other models may be fully explored.

- CHEA (Recognizes organization that grant accreditation to institutions of higher learning)
- DETC (Grants accreditation to particular institutions of higher learning)

See attachment 3 of addenda 2 for more details.

3. Public/Private Accreditation by Economic Sector (US Market)

This model is also highly evolved, and involved close coordination between governmental regulators and non-governmental accreditation. Given the quasi-governmental nature of this model and the nature of the long standing institutions to which it applies, it is not a clear fit for the EAP business case. However, various elements of the model are relevant and re-usable, as can be seen in the analysis of each in the last draft (attached).

- Banking (Chartering, Self-Assessment, Audit and Examination)(see:)
- Healthcare (Government licensing or permitting with private accreditation, e.g.: JCAHO)

See attachment 3 of addenda 2 for more details.

4. Internet Trust Marks

This model, relying heavily upon self-assessment and later verification on an as-needed basis by the licensor of the mark, has clear application to the EAP business case.

- TRUSTe
- ICRA

The basics of these models can be found in attachment 2 of addenda 2.

5. Circles of Trust

This model provides options that are most relevant to the "rules of engagement" and "closed community" aspects of the EAP endeavor. The examples in these models do not pertain especially to accreditation as generically understood, but all contain some criteria for admission that can be seen as comparable to certification. In addition, each model contains specific technical interoperability requirements and continued monitoring.

- NACHA/EBT
- SWIFT

The SWIFT Model can be found in the appendix to attachment 3 of addenda 2. The EBT model is under final drafting and will be appended shortly. The key document of the EBT model is the Operating Rules, which can be found at: http://ecitizen.mit.edu/EAP/RulesExamples/QUEST (along with other key documents). In short, the QUEST operating rules have legal force and effect based on contractual opt-in agreements by the parties using and servicing the EBT system. The liability for underlying transactions is spelled out in detail, as are the dispute resolution process and other legal terms. The parties are all represented on a governance board which is responsible for devising and revising the Operating Rules and related contracts and policies. Visa is another oft cited example of the closed system circle of trust. Another example is SecuritiesHub, (owned by Citigroup, Credit Suisse First Boston, Goldman Sachs, JPMorgan Chase & Co., Lehman Brothers, Merrill Lynch, Morgan Stanley, UBS Warburg, and Communicator Inc), and discussed in the White Paper "Online Gated Communities", available at: http://ecitizen.mit.edu/OnlineGatedCommunities/.

IV. Key Options Relevant to Each Model

1. Liability of the EAP. It appears to be common practice for an accreditor to disclaim all liability from those whom it accredits, as well as others certified by the accredited organizations or from end users of the certified products or services. There are some counter-examples of accreditation organizations that accept limited liability, such as the United Kingdom Accreditation Service (UKAS), such as for death or personal injury caused by UKAS' negligence.

2. Accreditation Criteria. It appears to be common practice for an accreditor to either refer to widely accepted international standards (such as ISO standards) and/or to develop criteria internally. Internally drafted criteria, such as the self-assessment survey by TRUSTe, are frequently revised in consultation with stakeholders. In closed system circles of trust, it is common for stakeholders to have a direct representation and vote on the operating rules which define the terms of the system, what parties may participate, liability and other terms. QUEST rules for EBT, the Operating Regulations of Visa, the governance and contractual documents enabling Securities.HUB, and the SWIFT rules are examples.

3. Dispute Resolution. It is common for dispute resolution to be handled by a senior executive committee of the accreditation organization (e.g. a committee of the Board of Directors). An appeals process is frequently spelled out, including the types of decisions that are appealable and the time frame within which a request must be lodged, argued and decided. In closed models, such as the EBT system, it is typical to see clauses requiring binding third party arbitration of commercial disputes.

4. Continuing Obligations. It is nearly universal that accreditation organizations require a) that the accredited organization warrant it shall remain in compliance for the period that it has been accredited, b) that the accreditor be advised of any material change in the status of the accredited organization, c) that the accredited organization consent to planned or surprise site visits, d) that self-assessments (less typically third party audits) be continually performed and submitted to the accreditor or available for inspection by the accreditor during the re-accreditation cycle, and/or that complaints by third parties (including end users) be sent to (directly or indirectly) the accreditor and that such complaints may form the basis of information leading to further assessment.

5. Consequences for Failure to Meet Obligations. The most typical explicit remedy for failure to remain in compliance with the accreditation criteria after accreditation has been granted is some combination of suspension, revocation or other modification (such as narrowing the scope of products or services to which accreditation applies) of the accreditation. In some cases, the accreditor may explicitly also reserve the right to notify third party regulators or law enforcement authorities, if, for example, the non-compliance threatens health or safety. There is also precedent for making general public announcements (e.g. on web site, perhaps via a press release, etc) of de-accreditation (see the ICSA blurb on "Validity Period" in attachment 3 of addenda 2).

6. Assessors. There is precedent for requiring self-assessment by the applicant for accreditation, against which in-house staff by the accreditor evaluate the applicant (such as TRUSTe and ICRA). There is also precedent for requiring direct site inspection by agents of the accreditor (Higher Education, UKAS, etc). And there is precedent for out-sourced sub-contracting of third party labs and assessors to evaluate an applicant for accreditation (such as with the UL family of labs and assessors).

7. Best Practices. Finally, the practice of posting all application materials, forms, complaint processes, and criteria on the web appears to be a best practice. The UKAS has also availed itself of a government MOU by which it holds a special legitimacy by declaration of government intent, though the MOU holds no legally binding weight. Having the accredited party pay all costs, as well as fees for accreditation is also a best practice. And, finally, it appears to be a best practice to use the application process as the key moment at which the applicant agrees contractually to all terms and conditions and related rules, incorporated by reference, to the application agreement.

V. Relevant Issues Raised by Each Model

The basic issues raised and addressed by each model group as follows:

1. Does the model apply to an organization that recognizes other organizations that will do the assessment and certification, or does the model apply directly to the process of assessment and certification?

2. What is the process of assessment? Is it conducted by: a) Self-Assessment, b) Third Party Audit (e.g. CPA), c) Assessors of the Accreditor, and/or d) Government examiners? Specifically, are there site-visits or not? What training is required of the assessors?

3. What are the criteria against which the product, service or organization is assessed, and where do they come from? For example, are they international standards (like ISO 9000), national standards (like the CHEA requirements for US accreditation of institutions of higher education), or unique requirements developed by the certification organization (like the TRUSTe Self-Assessment criteria)?

4. What is the role of continuing assessment and monitoring? Are periodic and/or surprise inspections part of the process? How deep and broad are the continuing assessment obligations and what is the cost of compliance? Are third parties (such as customers of the certified company) provided a means to communicate complaints to the accreditor?

5. What are the penalties for non-compliance? Under what circumstances is the certified party given an opportunity to cure the problem? Are there appeals or due process protections? Who decides appeals? What is the liability between the parties for serious harms that could result from mistaken granting or failure to grant certification, or misuse of certification?

6. What other business and legal rules apply to the certified companies or other parties and how are they supposed to be enforceable? Does the application process include a declaration or other acceptance of other rules? Are the rules incorporated by reference? To what extent do the rules specify rules applicable to third parties interacting with the certified company (such as students of the recognized college, consumers of the certified firewall, customers of the testing lab, and so on)? Is the certified company legally obligated to pass forward certain obligations or rights to its customers as part of the certification?

ADDENDA 1: Original Request for Service

Research and provide six (6) examples of existing Certification and Accreditation schema's that the EAP can utilize in determining the best model/approach for their own customization and adoption. The schema's can be from any vertical market and do not have to be specific to the identity management functional area.

Detailed information should be provided for each of the six sample schema. At a minimum, the following functional areas should be fully described in each of the schema:

* Functional Approach

o Is the schema model based on in internal or third party certification process?

* Example 1: Model owner directly conducts all certification/accreditation of identity issuers and replying parties

* Example 2: Model owner accredits a third party auditor to conduct assessments on their behalf, but maintains the process to provide final certification/accreditation of the identity issuers and relying parties

* Example 3: Any other model that are available to assess

o Define the decision making processes each model owner utilizes to develop and deploy their model

o Define the control/management processes each model owner utilizes to support their deployed model

o Define the liability framework associated with each named participant within the model, specifically as it applies to the certification and accreditation process

o Define the flow of money within the model, as it specifically applies to the certification and accreditation process (third party provider fees paid to the model owner for initial accreditation, third party continuing services/maintenance fees paid to the owner, identity issuer/relying party assessment fees paid to the third party auditor, identity issuer/relying party certification/accreditation fees paid to the owner)

o Define the dispute resolution process within the model, as it specifically applies to all named participants, within the certification and accreditation process

o Define the length of time that a third party auditor accreditation and/or identity issuer/relying party assessment and/or certification/accreditation would be valid for

The goal of this task is simply to collect six samples of differing certification and accreditation models that can be assessed from a functional, legal, business, technical, operational and maintenance/support perspective. EAP would like to review each of these six candidates and determine if one or more meet their perceived needs, customize as necessary and adopt for implementation.

/end/

ADDENDA B: Attachment of Previous Memos and Case Studies

ATTACHMENT 1:

Overview and Relevant Aspects of Internationally Recognized National Accreditation Models

The system seeks to enhance quality and cross-border recognition of accreditation and certification through the use of international standardization. In general, international bodies recognize national bodies which accredit organization that certify products or services. For example, the Underwriters Laboratory is accredited by the the American National Standards Institute which is the United States member of the International Standards Organization (as well as of the Interamerican Accreditation Cooperation organization and the International Accreditation Forum). Similarly, English product certification organizations are accredited by the United Kingdom Accreditation Service (UKAS), which is also a member of the ISO and IAF. Though the name is somewhat confusing, given that it is primarily a US organization accrediting US companies, the International Accreditation Services organization (IAS) is itself a member of the Interamerican Accreditation Cooperation (IAAC) which is recognized by the IAF.

Here is an example of the food-chain:

A. International Accreditation Organizations
- International Accreditation Forum (IAF) (http://www.iaf.nu/)
- International Standards Organization (ISO) (http://www.iso.org)
- Interamerican Accreditation Cooperation (IAAC) (http://iaac-accreditation.org/)

B. National Accreditation Organizations (recognized internationally)
- American National Standards Institute (ANSI) (http://www.ansi.org)
- United Kingdom Accreditation Service (UKAS) (http://www.ukas.com/)
- International Accreditation Services (IAS) (primarily US) (http://www.iasonline.org/)

C. Examples of Companies Conducting Certifications (Granting Certification to Products/Services)
- UL
- ICSA

Applicability

The reference to internationally and nationally recognized standards, as well as the basic application and accreditation procedures followed by the following two organizations appear largely applicable to the EAP base case. However, for purposes of the EAP, it would appear beneficial to substantially simplify and reduce the complexity and size of the endeavor and standards. In addition, the addition of EAP Business Rules in addition to accreditation and certification procedures would require a somewhat different business architecture. Nonetheless, the following processes and substantive rules are among the highest relevance of any examined during this research task. .

Example I
International Accreditation Service of Whittier, California
Scope Predominantly United States
http://www.iasonline.org/

IAS, formerly part of ICBO Evaluation Service, Inc, has been in operation since 1975. IAS operates as a nonprofit public benefit corporation that assesses and accredits competent testing and calibration laboratories, inspection agencies and fabricator inspection programs.

Basic Information:

Application Information for Companies Seeking Accreditation:
http://www.iasonline.org/PDF/Forms/index.html

Accreditation Criteria
http://www.iasonline.org/Accreditation_Criteria/index.html

Listing of Accredited Organization
http://www.iasonline.org/More/search.html

The Process of Accreditation by IAS

1. Application Submission

"Inspection agency" (aka "licensee" or "applicant") submits an application for accreditation. The application includes an authorized signature by the applicant and an agreement to: be bond by certain legal conditions (which, among other things, incorporate by reference the Rules of Procedure and the Accreditation Criteria, as amended from time to time).

A. Rules of Procedure. These include agreement to, among other things:
* Permit IAS to conduct "unannounced inspections" for which the licensee reimburses costs,
* The grounds for accreditation revocation or modification with a right to a hearing (including failure to comply with conditions in the application or for misstatements of fact, or " Any other ground considered as adequate cause in the judgment of IAS") and accreditation revocation/cancellation without the right to a hearing (including failure to pay required fees, failure to furnish required material or data, failure to respond to a deficiency report or to permit on-site inspection)
* The grounds for release of confidential data of the licensee by IAS (including pursuant to a court order)
* Permission to publish accreditation certificates on the IAS web site
* Refrain from referring to accreditation in any way that "indicates or implies" endorsement by IAS of any particular product.

B. Conditions for Application. This document, accepted by the licensee as part of the application, includes a long and detailed array of legal terms that strongly favor the accreditation authority, including:

* Reiteration of permission for spot inspection and reimbursements
* Comprehensive limitation of warranties:
  "…accreditation does not imply any guarantee or warranty, express or implied and including but not limited to any warranty of merchantability or fitness for any particular purpose, of any product tested or certified by the applicant, or any guarantee or warranty of any nature by IAS concerning any tests or calibration conducted by the applicant."
* Ceding various causes of action against IAS as the accreditor
  "Applicant agrees that it shall have no cause of action or claim against IAS, International Code Council (ICC), or any of their affiliates, parent, or brother or sister corporations or their Successors-in-Interest or assigns, or the officers, directors, members and employees thereof, arising in any manner from any denial of this application or from any accreditation given pursuant to this application, whether or not such accreditation is or is not subject to any conditions."
* Broad indemnity rights for IAS as the accreditor
  " Applicant agrees to hold IAS, ICC, and their affiliates, Successors-in-Interest, parent, or brother or sister corporations or their Successors-in-Interest and assigns, and the officers, directors, members and employees thereof of such entities harmless, and to protect, defend and indemnify them, with respect to any claim, liability, demand, action,

judgment, proceeding, costs, damages and expenses (including attorneys' fees) whether for personal injury, wrongful death, property damage, or any type of injury or damage whatsoever, arising from: (i) any certification or approval services of any nature provided by the applicant; (ii) the use of any service of any nature offered by the applicant, or the use or operation by any person of any product tested/calibrated or certified by the applicant, whether related to the matters set forth in the first sentence of this paragraph or otherwise; or (iii) the reference to or reliance upon, actual or asserted, any product certification or approval given by the applicant or any testing or calibration services rendered by the applicant including but not limited to the results of any testing or calibration conducted by the applicant.

* Favorable severability provision for IAS as the accreditor

" If any part or portion of this paragraph, or any application thereof to particular facts, should be determined invalid, the provisions hereof shall be severable so as to achieve for IAS and ICC the maximum legal application." and

* Incorporation by reference and agreement to other rules and procedures of IAS

" In consideration of the processing of this application, the applying laboratory agrees to abide and be bound by any conditions attached to any listing or renewal thereof issued pursuant to this application, or any later amendment of said listing or renewal, the Rules of Procedure for Laboratory Accreditation, which by this reference are made a part hereof, the Accreditation Criteria for Testing Laboratories, which by this reference is made a part hereof, and the Accreditation Criteria for Calibration Laboratories, which by this reference is made a part hereof, and any additions, deletions, or changes to such Rules or Accreditation Criteria hereafter adopted. In agreeing to abide and be bound by the Rules of Procedure and the Accreditation Criteria for Testing Laboratories and Accreditation Criteria for Calibration Laboratories, the applying laboratory understands that the failure to do so may result in the revocation, suspension or modification of accreditation issued pursuant thereto in accordance with the terms of the Rules of Procedure."

Highlighting the important status of this document, another signature and date are required at the bottom of the Conditions form, in addition to the signature required on the application which this form is a part of.

Along with the application, the applicant also submits the appropriate fees and a copy of the companies quality manual (against which it is assessed for accreditation).

2. Fees for IAS accreditation are as follows:

* New Applications (one year period of validity)
Range is between $1,000 (for Calibration Laboratories) to $5,950 (for Fabrication Inspection Programs of 76 employees and above).

* Renewal Applications (one, two and three year validity)
Somewhat less, but comparable to the application fees for new applications, with deeper discounts the more years purchased.

* Assessment Fee
Assessment fees in the $800/day range, as well as $600/day travel expenses are also applicable.

3. An IAS Representative is assigned to the application, and contacts the applicant to assist in bringing its manual "into full compliance with the accreditation criteria"

4. Once the manual is in compliance, the IAS staff will conduct on-site visits to the head quarters and field operations of the applicant. This is the assessment.

5. The management of the applicant is provided with an "assessment report" which may include "reference to corrective actions that must be carried out" in order to be accredited.

6. Accreditation is awarded once the applicant has taken any required corrective actions and satisfied all the other criteria.

7. Accreditation is granted for one year initially, and thereafter for one, two or three years. However, on-site inspections must happen no less than every two years.

Standards

IAS bases its standards upon ISO/IEC 17020: 1998, General Criteria for the Operation of Various Types of Bodies Performing Inspection. Unfortunately, this standard is proprietary and not available free of charge. A fee must be paid to the ISO to gain access to this document. This appears to be a relevant document and the EAP would benefit from gaining access to it.

IAS also develops its own standards and guidelines. For example, in a guidelines document clarifying requirements for "internal audit", IAS indicates the need for particular types of documentation, training of auditing staff, written procedures for corrective action in the case of problems discovered during audits, the minimum time periods between internal audits and other relevant factors. Another document clarifies which personnel with signatory authority for test and assessment results are sufficiently significant to trigger a need to notify IAS when there are personnel changes in those roles. Many other guidelines and clarifications are also provided by IAS to assist the companies it accredits.

Example II
United Kingdom Accreditation Service of Feltham, UK
Scope Predominantly United Kingdom
http://www.ukas.com/

The United Kingdom Accreditation Service (UKAS) is the sole national accreditation body recognised by government to assess, against internationally agreed standards, organisations that provide certification, testing, inspection and calibration services. Accreditation by UKAS demonstrates the competence, impartiality and performance capability of these evaluators.

Basic Information:

Application Information for Companies Seeking Accreditation:
http://www.ukas.com/information_centre/accreditation_category_forms.asp

Accreditation Standards
http://www.ukas.com/about_accreditation/accreditation_standards.asp
http://www.ukas.com/information_centre/publications.asp

Listing of Accredited Organization
http://www.ukas.com/about_accreditation/accredited_bodies/default.asp

The Process of Accreditation by UKAS

1. Application Submission

Applicant (aka "licensor" or "accredited organization") submits an application for accreditation. It can take, typically, between half a year and a year and a half to achieve accreditation from the date of application, depending on the type of accreditation sought and the size/complexity of the applicant organization and process.

The application includes a "declaration" page, whereby the applicant agrees to "comply with the relevant European or International Standards, the applicable UKAS requirements, and UKAS Publications as listed on the website (www.ukas.com)." In this way, the various policies, procedures and other rules are incorporated by reference into the application process itself, with binding effect.

The declaration page also requires indication that two signed copies the the UKAS Agreement are enclosed with the application, along with the non-refundable £1200+VAT application fee. The signature line includes a warranty that the signatory is authorized to sign for the applicant and that all the information in the application is "correct and accurate to the best of my knowledge and belief."

The UKAS Agreement, signed and enclosed with the application, is an excellent and relatively balanced set of terms governing the entire accreditation process, including the following terms:

* *Surprise Inspection.* UKAS reserves the right to carry out additional or unscheduled surveillance visits, as it may reasonably require.

* *Discretionary revocation, suspension or other sanctions, if applicant fails to cure problem.* If, in UKAS' view, the applicant fails to comply with the terms of this Agreement, UKAS may suspend or withdraw accreditation, reduce the scope of accreditation, impose a moratorium on the issue of accredited certificates or extensions to scope, require re-assessment or impose such other sanctions as are appropriate and legal. Withdrawal of accreditation will not be imposed unless the Body fails to carry out the actions required to maintain accreditation in the requisite timescales as notified in writing by UKAS.

* *Warranties to cooperate with business rules.* Applicant makes warranties it provides accurate, complete information, will open facilities for inspection, will remain in compliance with rules at all times, will notify UKAS of planned material changes (which are listed in the agreement), will "Not to use its accreditation in such a manner as to bring accreditation into disrepute", and will "make it clear in all contracts with its clients and in guidance documents that a certificate or report issued by it in no way implies that any product, service or management system certified is approved by UKAS.

* *Promise to help investigate and resolve third party complaints.* "To assist UKAS in the investigation and resolution of any properly authenticated complaints made by third parties about the Body's accredited activities."

* *Confidentiality.* Agreement to keep applicant information confidential, except in cases such as a court order.

* *Relatively even-handed mutual liability and damages allocation, and exceptions*. "In providing the service(s), information or advice, neither UKAS nor any of its officers, employees or agents warrants the accuracy or completeness of any information, review, audit, accreditation or advice supplied. Except in respect of death or personal injury caused by UKAS' negligence or as set out herein, neither UKAS nor any of its officers, employees or agents (on behalf of each of whom UKAS has agreed this clause) shall be liable to the Body for any loss of profit or any indirect, special or consequential loss, damage, costs or expenses or other claims (whether caused by the negligence of UKAS, its officers, employees or agents or otherwise) which arise out of or in connection with the provision of the services or their use by the Body by reason of any representation (unless fraudulent) or any implied warranty, condition or other term, or any duty at common law or under the express terms of this Agreement, and the entire liability of UKAS under or in connection with this Agreement shall not exceed the higher of £25,000 or the agreed annual fee."

* *Limited indemnity for the UKAS only for misuse of accreditation or breach by applicant.* "The Body undertakes to indemnify UKAS against any losses suffered by or claims made against UKAS as a result of misuse by the Body of any Certificate of Accreditation or licence to use any accreditation mark granted by UKAS or as a result of any breach by the Body of the terms of this Agreement."

* *Simple 90 day-notice mutual termination clause.* And,

* *Prohibition against assignment absent written agreement by the parties.*

2. Fees for UKAS accreditation are as follows:

Application Fee
The fee is £1200 (£1410 including VAT)

Daily Rate for Pre and Initial Assessment Work
The daily rate for pre -assessment and initial assessment work is £775.

Daily Rate for Other Work
The daily rate for all other services, unless otherwise agreed, is £542.

Annual Accreditation Fees
The fee is calculated as a quarter of the total assessment effort in the four year program multiplied by the day rate for the standard set out below

Standard	£
ISO/IEC 17025, ISO/IEC Guide	43 83
ISO/IEC 17020	260
EN 45011/45012, ISO/IEC 17024, ISO/IEC Guide 66	285

A pro-rata fee will be charged if accreditation is granted during the year.

3. Application Received, Staff Allocated

Upon receipt, the application is reviewed by an Accreditation Manager who allocates an Assessment Manager to the case. The Assessment Manager is the case officer responsible for taking the applicant through the accreditation process and for maintaining and renewing accreditation in the future.

4. Applicant Contacted

The Assessment Manager contacts the applicant after studying the documentation submitted and discusses the need for a pre-assessment visit and the composition of the proposed assessment team.

5. Pre-assessment Visit, Provision of Firm Quote

UKAS normally recommends a pre-assessment visit by the UKAS Assessment Manager. This visit addresses the scope of accreditation requested and will normally involve between 1 and 3 man-days work. It is designed to confirm the applicant organization's readiness for full assessment. The Assessment Manager provides a quotation for the work involved.

6. Initial Assessment Visit

This is conducted by the Assessment Manager supported, as necessary, by technical assessors with the expertise to cover the scope of accreditation. The length of the visit will depend upon the scope of accreditation requested. Prior to the visit, the applicant receives a "visit plan" which provides a proposed timetable for the work to be assessed. Any nonconformities found against accreditation requirements are notified to the applicant in writing during or immediately following the assessment visit.

7. Granting of Accreditation and Renewal Periods

After being apprised of nonconformities, the applicant is then asked to advise UKAS on how it intends to clear the nonconformities. Once they have been cleared to the satisfaction of UKAS, applicant is granted accreditation. Accreditation is "confirmed on an annual basis by surveillance visits, with a full re-assessment every fourth year. The first surveillance visit takes place 6 months after the Grant of Accreditation."

Standards

The UKAS also relies upon ISO standards that are proprietary. In addition, however, it relies upon various highly relevant European standards that are freely available in English. One such key standard is EA-7/01, The EA Guidance on the application of ISO/IEC Guide 62:1996, and EA-7/03, EA-6/02, EA 6-01, and other EU and UKAS standards and guidelines available at http://www.ukas.com/information_centre/publications.asp.

MOU

Another interesting and relevant aspect of the UKAS example is the presence of an MOU between it and the government of the UK. The MOU is available at: http://www.ukas.com/about_UKAS/memorandum_of_understanding.asp. This document is interesting because it exists solely in the realm of perception and trust and (by its own terms) it " does not create any rights, liabilities or obligations which would have binding effect in law." However, the UK government does use the non-binding language to communicate the UKAS is the "sole national body in the UK recognised by Government to provide accreditation of conformity assesment…" and indicates a willingness to encourage government and private organizations to use the services of UKAS and to provide public funds if needed to assist in creation of new accreditation services until they are self-funding. Though the document has no binding legal effect, it is a powerful message to organizations across the economy about the legitimacy and importance of the accreditation process and UKAS.

/end/

ATTACHMENT 2.

MODEL BLURB	**WHO: TRUSTe** WHAT: Internet Privacy Certification and Trust Mark Issuance URL: http://www.truste.org/
Internal or 3rd Party Assessors	Mix of Self-Assessment and final check by TRUSTe staff. Right to on-site inspection by CPA or other party is reserved, for cause (e.g. patterns of complaints).
Decision Making Process	The criteria appear to be developed by TRUSTe itself, in consultation with "consumers and government authorities".
Control and Mgmt. Processes	In the first instance, applicants for the privacy seal agree to a license agreement with many legal term and obligations, including submission of a truthful self-assessment of the companies privacy practices. The self-assessment is submitted and TRUSTe staff verified the information with the company typically (evidently) by talking on the phone with company staff and looking at the companies web site and other information. It is not part of the regular course of business to make a site visit to the company, but the right to do so is reserved by TRUSTe, for cause. "Once TRUSTe has processed your application, received your privacy statement, and obtained a completed self-assessment form, your account manager will contact you to set up a phone conference to review your site and privacy statement. For Web sites that have not launched yet, please keep in mind that you will need to provide TRUSTe access to the site for us to conduct our review and certification process."
Liability of Each Party	The liability of TRUSTe and companies that have been approved to use the TRUSTe privacy seal is detailed in the License Agreement, including: * A full warranty disclaimer by TRUSTe, * Indemnity by TRUSTe to licensee in event of IP infringement suit based on TRUSTe mark, * Indemnity by licensee to TRUSTe for a wide range of other potential sources of litigation based on use of the TRUSTe mark, * complete mutual waiver of consequential, indirect, incidental, punitive damages or damages from lost profits, or damage to good will, and * Liability limitations of the total amount actually paid apply to each party vis each other, except for damages, losses, expenses, and other costs to TRUSTe for misrepresentations by licensee. Note: the above is a simplification of the key legal terms. Also, there are more varied and detailed terms bearing on liability of parties.
Flow of Money	Pricing for companies with a single brand: **Your Company's Annual Revenue in USD** — **Cost Per Brand** $0 - $4,999,999 — $599 $5,000,000 - $9,999,999 — $899 $10,000,000 - $19,999,999 — $1,999 $20,000,000 - $49,999,999 — $3,999 $50,000,000 - $74,999,999 — $4,999 $75,000,000 - $99,000,000 — $6,999 $100,000,000 - $499,999,999 — $8,999 $500,000,000 - $1,999,999,999 — $9,999 $2,000,000,000 and above — $12,999

	Corporate (up to 10 brands) $25,000 Enterprise (up to 300 brands) $75,000 Pricing for companies with multiple brands: The **$25,000 Corporate** and **$75,000 Enterprise** rates are for companies with multiple brands that all share a common privacy policy and adhere to common information collection practices.
Dispute Resolution Process	There is an appeal process for approval/non-approval decisions with decision by 2 privacy experts and 2 members of the TRUSTe Board of Directors. In addition, TRUSTe provides "watch dog" services to consumers with complaints about privacy practices of companies licensed to use the TRUSTe privacy seal. Evidently, TRUSTe attempts to help negotiate solutions and reserves the right to the following remedies:
Validity Period of Cert-ification	One or Two years. However, " licensees will submit a full self-assessment every three years, regardless of the length of their license term (with exceptions, e.g., in the case of an assignment or when the Program Requirements have changed). COPPA and EU Safe Harbor program participants must continue to complete a new self-assessment annually, in keeping with the specific requirements of those programs."
Notes/Ideas	Again, the ability to field complaints directly from customers of the company certified appears to be a major component of the reliability and assurance regime.
Parking Lot	

MODEL BLURB	**WHO: Internet Content Rating/ICRA** What: Self regulatory parental ratings online system. URL: http://www.icra.org/
Internal or 3rd Party Assessors	Self-Ratings by licensee of ICRA mark, with automated and manual checks to verify accuracy of rating.
Decision Making Process	ICRA as a non-profit corporation evidently makes final determination of the criteria. In this case, the criteria are content classifications (e.g. regarding nudity, violence, language, etc).
Control and Mgmt. Processes	A licensee submits an online application to become an Associate member or contacts staff directly to inquire about full membership. Membership evidently requires agreement to Terms and Conditions and other legal provisions covering the ratings and compliance process. The ICRA reserves the rights to conduct manual checks of content compliance in addition to the usual automated checking processes.
Liability of Each Party	The legal pages associated with the membership form indicates the Licensee agree: * not to impair the title, rights or interests of the ICRA in the ICRA marks (e.g. by registering the mark or using a confusingly similar mark), * " indemnify and hold ICRA™ harmless from any claims, suits, losses or damages (including reasonable legal fees incurred by ICRA), arising as a result of breach of this agreement or any other action taken by you in connection with any services, labelled site, misrepresentation, or violation of the registration questionnaire." * enter into this agreement without any representation or warranty of any kind being made by ICRA * actions by the ICRA " shall not give rise to any liability or obligations on the part of ICRA, or any rights of reliance by or for you or any third party, nor otherwise be deemed or construed as being for the benefit of

	you or any third party. ICRA does not warrant or guarantee that the label will not infringe the trademark, service mark, trade name, copyright, or other intellectual property rights of any third party." NOTE: there does not appear to be any requirement that the licensee have a contract in place with others absolving the ICRA of liability to them or other third parties.
Flow of Money	Membership Categories and Subscription Levels Annual Subscription in US dollars Euros and Sterling (in that order): Corporations (With more than 100 employees) 30,000 35,650 21,350 Corporations (Fewer than 100 employees) 15,000 17,825 10,675 Non-profit (More than 100 employees)* 30,000 35,650 21,350 Non-profit (Fewer than 100 employees) 5,000 5,940 3,560 Associate member 100 100 70 * ICRA Board may waive a portion of the fee
Dispute Resolution Process	There does not appear to be a formal dispute resolution process in place. However, in the event of revocation of a license because of misrepresentation of content, notification is sent to the licensee. "If the situation is not remedied two weeks after such notification ICRA reserves the right to take appropriate action including but not limited to, making the misrepresentation known through lists, web-postings and notifications to the press."
Validity Period of Cert-ification	Apparently the validity period runs with the dues period, which is annual.
Notes/Ideas	The concept of automated testing, while clearly relevant to use of the filters and other standards applied by ICRA, may also have useful application for the EAP. Services of providers, use or validation of an EAP credential and other aspects of the work flow of the EAP system may be capable of processing and testing by automated means.
Parking Lot	

ATTACHMENT 3.

Accreditation, Certification and Assessment Models

Prepared by Daniel Greenwood, Esq. for the EAP
May 27, 2004

Introduction

This overview is a partially complete analysis of research into several accreditation, certification and assessment models of potential application to the EAP. Not all models have been analyzed, and some are only partially complete. Attached at the end of the document are some preliminary summaries of some of the models done by research affiliates of mine and from which I am drawing basic references and links. I attach these summaries for your reference only, but they have not been fact checked and are not finished or presented work on this assignment.

Next steps are to finish analyzing the research and complete filling out the grid. Then, to look across each of the models in detail and evaluate similarities, differences and ideas drawn form each model.

Notes on grid nomenclature:

* Information in brackets is tentative and based on apparent or probable facts, but not yet independently confirmed or traceable to a citation.

* The phrase "decision making process" is applied primarily to the decisions regarding testing criteria. Other decision making, such as management, governance or corporate decisions are treated in the block for Control and Management Processes.

* Not all information for all models are yet complete. Background information on many of the models can be found, in cached form (to guard against network unavailability at the source) at: http://ecitizen.mit.edu/EAP/Accreditation/raw-research/ as well as through the links provided in the grids.

* The "Parking Lot" item is reserved for particular issues, problems or prospects that arise in discussion a given model, but which must be returned to later in order to move forward with the bulk of the work in a timely manner. (In effect, they are put in the lot for later).

* In no particular order, (in the form "Topic/Name") these are the Models currently being examined:

- IT Security Products/ICSA
- Network Administrators/Microsoft MSCE, Novell CNE
- Higher Education/CHEA&DETCA
- Electronics/UL
- Computer Security Labs/NIST
- Banks(FDIC)/Self Assessment Mix With Audit/Regulation
- Hospitals/JCAHO
- Internet Content Rating/ICRA
- Global Payments/SWIFT
- EMortgage eAuthentication/SISAC
- National Accreditation Scheme (Germany)/DAR

Uniform Grid of Accreditation, Certification and Assessment Model

MODEL BLURB	**Who: ICSA.** What: Certification of Firewall. URL: http://www.icsalabs.com/html/communities/firewalls/index.shtml
Internal or 3rd Party Assessors	Model Owner Assesses and Certifies the firewall products. "Certification testing is performed either by skilled ICSA Labs security analysts or by third-party lab analyststs trained and authorized by ICSA Labs for this purpose. As a design goal, testing is automated where possible, and is checklist oriented where not automated. The test procedures are reproducible, objective and not open to interpretation whatsoever. The testing personnel or authorized labs must have access to the product's associated help-desk, or the system's security personnel, to resolve questions. And there is an escalation procedure to resolve any potential conflicts or judgment questions." http://www.icsalabs.com/html/certification/index.shtml
Decision Making Process	Criteria used is developed by ICSA itself. Vendors of certified products are invited to join the Firewall Product Developers Consortium (FWDC) as a way to "influence" the process and criteria. " To develop and evolve appropriate and meaningful certification criteria, ICSA Labs uses a "notice of proposed certification criteria" system. ICSA Labs queries numerous specialists and organizations, potentially including affected vendors, developers, and users; the security expert community, the non-vendor specialists and experts, the Fortune-500 and vertical user consortia, unrelated or minimally related vendor consortia, academia, and other consumer and industry groups. A draft proposed criteria is then circulated within the appropriate people and groups before making the criteria final. Finally, ICSA Labs Certification criteria and processes are overseen by a Certification Oversight Board made up of well known security experts, which itself has broad representation."
Control and Mgmt. Processes	[Corporate lines of control internal to ICSA. Further information pending.]
Liability of Each Party	* ICSA secures contractual obligation by vendors to maintain their Certified products "that the product or system will be maintained at the current, published ICSA Labs Certification standards." Failure to meet this obligation, e.g. as identified during a spot test, leads to de-Certification (see Validity Period). * According to the site's FAQ, ICSA maintains an NDA with vendors seeking certification that precludes disclosing whether a vendor failed to achieve certification. Presumably, there is contractual liability for failure to meet these confidentiality obligations between ICSA and the vendors. Beyond this, no further information is available at this time. * ICSA publishes extensive information on avoiding Anti-Trust liability on its web site, called "ICSA Labs Anti-Trust Guidelines".
Flow of Money	Vendor pays for certification Vendor pays membership in Consortium (separate from certification) Customers view certification lists at no charge.
Dispute Resolution Process	Not available. [ICSA Labs urges vendors to be involved in the process of setting product standards. Then it urges vendors to patch or upgrade their products that fail the testing process. If a product is not performing to standard, ICSA communicates with the vendor's customer service people to see if they can remedy the problem.]
Validity Period	Approximately one year. However, spot testing is authorized. Failure

of Cert-ification	to remedy flaws discovered during spot test lead to public revocation of Certification. "If the shipping product or production system still does not meet current certification criteria by the end of this grace period, then ICSA Labs Certification is explicitly and publicly revoked." http://www.icsalabs.com/html/certification/index.shtml
Notes/Ideas	Accreditation is not used as a word, "Certification" is used to mean the process of testing a product leading to decision on whether it may use the ICSA trust mark (i.e.: is a "Certified firewall"). ICSA offers membership as way to influence development of criteria by vendors on a vendor consortium. This is a different model from membership in a stakeholder council that makes the final decisions and is partially comprised of vendors (i.e.: CSPs) who are also the subject of Certification. ICSA method eliminates potential appearance of conflicts of interests. However, it also eliminates collaborative partnership benefits.
Parking Lot	

MODEL BLURB	**Who: Council for Higher Education Accreditation** What: Recognition of Higher Education Accreditators. CHEA "Recognizes" (i.e.: accredits) organizations that themselves Accredit institutions of higher education (such as the DETCA, below). URL: http://www.chea.org
Internal or 3rd Party Assessors	Model owner assesses organizations applying for recognition. CHEA "Committee on Recognition" is appointed by the CHEA Board of Directors. Committee membership is staggered and drawn from various stakeholder groups and is accountable to the Board. In discretion of the Committee, "peer review" may be added to assessment, whereby, in consultation with organization seeking recognition, a "site visitor" may be selected to perform an on-site inspection.
Decision Making Process	The criteria against which applicants for recognition are assessed are wholly developed by CHEA. See: http://www.chea.org/recognition/recognition.asp
Control and Mgmt. Processes	A detailed process is set out involving a "Self-Study" application (basically, self assessment against the criteria), back and forth between the Committee and applicant in written form, a possible site visit, a public presentation, opportunity for comments, and ability to seek decision review. Notice is built in at nearly every phase. The Board of Directors exercises ultimate ownership and control over the decision process, but the Committee is invested with authority to act based on the rules.
Liability of Each Party	Unknown at this time.
Flow of Money	The applicant for recognition pays all costs of recognition, including direct costs, annual participation fee, and other costs. There are also membership dues, sponsorships, fees for accreditation visits, conference revenue and other sources of funding for CHEA. See: http://www.chea.org/pdf/fact_sheet_5_operation.pdf and http://www.chea.org/recognition/recognition.asp#24
Dispute Resolution Process	This is addressed at three levels: 1. Accrediting organizations seeking recognition from CHEA may seek review and appeal of a negative decision by the Recognition Committee,

	2. Accrediting organizations must have mechanisms by which an institution or program that is dissatisfied with a review may express its dissatisfaction and seek redress, and 3. Accrediting organizations describe the terms and conditions under which a complaint can be lodged against an institution or program that is accredited (this includes complaints from the general public, by students or others).
Validity Period of Certification	For a maximum of 10 years, with a five year interim report, but CHEA may review at any time "if the accredit or makes major changes in how it operates or if there are a series of documented concerns about the organization." http://www.chea.org/pdf/fund_accred_20ques_02.pdf
Notes/Ideas	
Parking Lot	

MODEL BLURB	**Who: Distance Education and Training Council** What: Accreditation of Institutions of Higher Education Using Distance Learning Technologies URL: http://www.detc.org/
Internal or 3rd Party Assessors	[Model owner directly assesses applicant institutions, including through use of on-site inspections]
Decision Making Process	[Model owner determines criteria and posts all relevant information on its web site.]
Control and Mgmt. Processes	[Model owner accreditation team, using self-appraisal information and site-visits, test applicant against criteria.
Liability of Each Party	[Contractual obligations by applicant educational institution promising, among other things, to notify DETC of material changes and not to publish fact of accreditation in progress so as to avoid misleading the public as to accreditation status.]
Flow of Money	[Applicant pays all costs according to a published fixed cost schedule for site visits and other activities. Typical accreditation fee is $7,000 - $10,000 USD]
Dispute Resolution Process	[Process published to contest decision of DETC, but appeal is made to DETC, with due process protections in place. Also, process for third party complaints to DETC regarding accredited institutions is in place and publicized.]
Validity Period of Cert-ification	[There are five-year re-accreditation reviews, with immediate status review when cause shown.]
Notes/Ideas	This is a very good model in terms of detailed practices and policies including many potentially useful ideas. All their processes and rules are available for free online.
Parking Lot	

MODEL BLURB	**WHO: Underwriters Laboratory** WHAT: Certification of Products Safety and Quality URL: http://www.ul.com
Internal or 3rd Party Assessors	Model owner tests products in UL Labs or other authorized labs in the "family of companie", and also conducts follow-up visits to test products after certification in the field. **60** laboratory, testing and certification facilities were part of the UL family of companies. UL staff examine how products

	are constructed, conduct tests, evaluate results and develop safety standards. UL also has field representatives who visit manufacturers' facilities. They help confirm that products bearing the UL Mark comply with applicable UL safety requirements. UL conducted **547,708** follow-up visits in 2003 to audit compliance with product certification requirements. In addition, apparently UL has an MOU in place allowing other organizations to test to UL Safety Standards. " The UL family of companies maintains a number of agreements, called Memorandums of Understanding (MOUs), with product testing and certification organizations in international markets. The MOU provides a mechanism for the two participating agencies to work toward mutual recognition of each other's testing results for one or more specific product categories."
Decision Making Process	Model owner determines criteria. " UL Standards for Safety are developed under a procedure which provides for participation and comment from the affected public as well as industry. The procedure takes into consideration a survey of known existing standards and the needs and opinions of a wide variety of interests concerned with the subject matter of the standard. Manufacturers, consumers, government officials industrial and commercial users, inspection authorities and others provide input to UL." There are **876** UL Standards.
Control and Mgmt. Processes	Details not yet available. Evidently, there is a somewhat collaborative process whereby a company submits an application for testing, and is consulted as to the testing process, fees, scope, timing and other aspects during an initialization period.
Liability of Each Party	Details not yet available. [There may be some potential benefit in terms of evidence of non-negligence in judicial proceedings if a defendant can show certification by and compliance with UL standards in a product liability or other tort action. In addition, there are legal confidentiality requirements in the application contracts whereby applicant proprietary or trade secret information is kept confidential and UL employees sign NDA's to assure applicant information remains confidential.]
Flow of Money	Details to follow. "Cost varies depending on the product and complexity of test requirements. Once UL's engineering staff review your product information to determine the scope and time involved in the testing process, they will provide you with a cost estimate. UL will work with you in determining the time frame for testing, depending on when you need the project completed."
Dispute Resolution Process	There is some form of an internal appeals process for UL rejection of certification that, evidently, does not affect other aspects of the UL/applicant relationship. " If you have any questions about your test results, the interpretation of a requirement or any UL decision, the UL appeals procedure provides a method for your concerns to be heard by UL management without jeopardizing your relationship with UL. Just contact our engineering staff for more details." In addition, there are processes documented in the UL site FAQ regarding "Variations" (i.e. when a product is found not to comply after certification has been granted). To resolve the items written on the Variation Notice, the manufacturer can elect one of the following choices for each item: • Rework the units to bring them into compliance, • Remove the UL Mark from the affected units, or

	• Hold the units pending review by UL. So called "variations" can result in withdrawal of the authorization to use the UL Mark.
Validity Period of Cert-ification	Details not yet know. [Evidently, it is perpetual, with follow-up inspections paid for by applicant. "You must agree to participate in UL's Follow-Up Services program. You indicate your willingness to participate by signing and returning the Follow-Up Services Agreement."] There are a large number of different UL marks, each signifying different compliance or a different market (see: http://www.ul.com/mark/index.html)
Notes/Ideas	The relatively collaborative nature of the relationship between applicants and the UL lab staff who will conduct the testing was a surprise. Evidently, this somewhat flexible process has not negatively affected the quality or perceived reputation of the UL process.
Parking Lot	

MODEL BLURB	WHO: TRUSTe WHAT: Internet Privacy Certification and Trust Mark Issuance URL: http://www.truste.org/
Internal or 3rd Party Assessors	
Decision Making Process	
Control and Mgmt. Processes	
Liability of Each Party	
Flow of Money	
Dispute Resolution Process	
Validity Period of Cert-ification	
Notes/Ideas	
Parking Lot	

MODEL BLURB	Network Administrators/Microsoft MSCE, Novell CNE (http://www.novell.com/training/certinfo/ http://www.microsoft.com/learning/mcp/mcse/default.asp)
Internal or 3rd Party Assessors	
Decision Making Process	
Control and Mgmt. Processes	
Liability of	

Each Party	
Flow of Money	
Dispute Resolution Process	
Validity Period of Cert-ification	
Notes/Ideas	
Parking Lot	

MODEL BLURB	Computer Security Labs/NIST http://csrc.nist.gov/sec-cert/ca-process.html and http://csrc.nist.gov/nissc/1998/proceedings/paperE1.pdf
Internal or 3rd Party Assessors	
Decision Making Process	
Control and Mgmt. Processes	
Liability of Each Party	
Flow of Money	
Dispute Resolution Process	
Validity Period of Cert-ification	
Notes/Ideas	
Parking Lot	

MODEL BLURB	Banks(FDIC)/Self Assessment Mix With Audit/Regulation (See, generally, http://ecitizen.mit.edu/EAP/Accreditation/raw-research/BANKS/Research/)
Internal or 3rd Party Assessors	
Decision Making Process	
Control and Mgmt. Processes	
Liability of Each Party	
Flow of Money	
Dispute Resolution Process	

Validity Period of Cert-ification	
Notes/Ideas	
Parking Lot	

MODEL BLURB	Hospitals/JCAHO http://www.jcaho.org
Internal or 3rd Party Assessors	
Decision Making Process	
Control and Mgmt. Processes	
Liability of Each Party	
Flow of Money	
Dispute Resolution Process	
Validity Period of Cert-ification	
Notes/Ideas	
Parking Lot	

MODEL BLURB	Internet Content Rating/ICRA http://www.icra.org/
Internal or 3rd Party Assessors	
Decision Making Process	
Control and Mgmt. Processes	
Liability of Each Party	
Flow of Money	
Dispute Resolution Process	
Validity Period of Cert-ification	
Notes/Ideas	
Parking Lot	

MODEL BLURB	Global Payments/SWIFT http://www.swift.com/
Internal or 3rd Party Assessors	
Decision Making Process	
Control and Mgmt. Processes	
Liability of Each Party	
Flow of Money	
Dispute Resolution Process	
Validity Period of Cert-ification	
Notes/Ideas	
Parking Lot	

MODEL BLURB	EMortgage eAuthentication/SISAC http://www.sisac.org/
Internal or 3rd Party Assessors	
Decision Making Process	
Control and Mgmt. Processes	
Liability of Each Party	
Flow of Money	
Dispute Resolution Process	
Validity Period of Cert-ification	
Notes/Ideas	
Parking Lot	

MODEL BLURB	National Accreditation Scheme (Germany)/DAR http://www.dar.bam.de/qmh_e/
Internal or 3rd Party Assessors	
Decision Making	

Process	
Control and Mgmt. Processes	
Liability of Each Party	
Flow of Money	
Dispute Resolution Process	
Validity Period of Cert-ification	
Notes/Ideas	
Parking Lot	

Accreditation and Certification Potential Matix

[Note: It remains to be seen how meaningfully to capture information in each cell. However, this is a draft matrix in a proper form to do a single comparison chart.]

Name	Internal or 3rd Party Assessors	Decision Making Process	Control and Mgmt. Processes	Liability of Each Party	Flow of Money	Dispute Resolution Process	Validity Period of Cert-ification
FDIC	Mixed	Gov't	Gov't	Complex	UserPays		
JCAHO							
ICRA							
ICSA							
SWIFT							
CHEA							
DETC							
SISAC							
UL							
TRUSTe							

APPENDIX: Raw Research Summaries

Model name: Combination self-assessment and external examination

Representative of the model: US National Banks

Summary: A chartered bank must satisfy standards established by a third party, namely regulators such as the Office of the Comptroller of the Currency, the FDIC and the Federal Reserve. To meet those standards, a bank hires executive officers to manage the bank in accordance with the standards. A bank must set up a board of directors and an internal audit function that monitors compliance constantly. The board of directors and internal auditors do the lion's share of the accreditation work. Next, building on the work performed by the board of directors and the internal auditors, external CPA auditors examine the bank periodically. The internal auditors and external auditors must be independent of each other. See Interagency Policy Statement on Internal Audit and Internal Audit Outsourcing, March 17, 2003, OCC 2003-12. Then, building on the work of the internal and external auditors, third-party examiners (from government regulators) examine the bank. See "About the OCC" at http://www.occ.treas.gov/aboutocc.htm.

Is the schema model based on in internal or third party certification process?

The model is based on a combination, including both internal and third party review. The third-party component includes review by both an external CPA and a third party regulator. In a variation of the model, the third party regulator could be replaced by a private industry association.

Define the liability framework associated with each named participant within the model, specifically as it applies to the certification and accreditation process.

By law, the executive officers and the board of directors assume liability to investors, depositors and other creditors. In theory, internal auditors assume professional liability, but in practice they are sued only in extreme circumstances; internal auditors are usually just mid-level employees. The external CPA auditors assume a measure of professional malpractice liability. The third party regulator (or industry association) assumes no liability, but it has a reputation to uphold.

Define the flow of money within the model, as it specifically applies to the certification and accreditation process (third party provider fees paid to the model owner for initial accreditation, third party continuing services/maintenance fees paid to the owner, identity issuer/relying party assessment fees paid to the third party auditor, identity issuer/relying party certification/accreditation fees paid to the owner).

The bank pays

* salary to the executive officers
* fees to the members of the board of directors,
* salary to the internal auditors,

* fees to the external auditors
* periodic dues to the third party regulator (regarding dues to the Office of the Comptroller of the Currency, see "About the OCC" at http://www.occ.treas.gov/aboutocc.htm).

Define the dispute resolution process within the model, as it specifically applies to all named participants, within the certification and accreditation process.

Those parties identified above as bearing liability can be sued by investors, depositors and other creditors of the bank.

The bank can fire the directors and auditors with which it disagrees. If a bank disagrees with an examiner, the bank has right to appeal within the regulatory framework governing the examiner.

Define the decision making processes each model owner utilizes to develop and deploy their model.

The standards are established by regulators in consultation with the banks and the public. Regulators are constantly reviewing their standards and revising them. To meet the standards, the bank board of directors is responsible for authorizing and monitoring internal measures. The executive officers are responsible for implementing internal measures.

Define the control/management processes each model owner utilizes to support their deployed model.

Regulators possess a range of sanctions they can bring against banks that fail to comply, including fines, changes in capital requirements and the power to bar individuals from serving as bank officers.

The results of regulatory examinations are normally not made public, although the FDIC does publish some quarterly information about each bank's financial condition. see "About the OCC" at http://www.occ.treas.gov/aboutocc.htm.

Define the length of time that a third party auditor accreditation and/or identity issuer/relying party assessment and/or certification/accreditation would be valid for.

A bank's status can change almost immediately. Regulatory examination and discipline can occur at any time.

The goal of self-assessment by the board of directors and internal audit is to ensure constant compliance with standards and real-time correction when a deviation occurs.
Model name: Honor system labeling

Representative of the model: Internet Content Rating Association

Summary:

"The Internet Content Rating Association is an international, independent organization that empowers the public, especially parents, to make informed decisions about electronic media by means of the open and

objective labelling of content. . . . Web authors fill in an online questionnaire describing the content of their site, simply in terms of what is and isn't present. ICRA then generates a Content Label (a short piece of computer code) which the author adds to his/her site.

"Users, especially parents of young children, can then set their internet browser to allow or disallow access to web sites based on the objective information declared in the label and the subjective preferences of the user." http://www.icra.org/_en/about/

In large measure, the ICRA model is a voluntary honor system.

"ICRA makes both automated and manual checks on sites to verify that labels are in place and that they are applied appropriately." http://www.icra.org/_en/webmasters/#matrix

Is the schema model based on in internal or third party certification process?

A web site wishing to participate reviews its web content and then labels it in accordance with the ICRA terms and guidelines. ICRA monitors use of its label primarily through automated and artificial intelligence searches. ICRA can conduct manual inspections. And, as an additional level of review, ICRA invites complaints from the public.

Define the liability framework associated with each named participant within the model, specifically as it applies to the certification and accreditation process.

"Displaying an ICRA logo button or 'Labelled with ICRA' text link without carrying the label is a breach of our terms and conditions." http://www.icra.org/_en/webmasters/#matrix

The ICRA labelling and filtering systems are protected by the U.S. Copyright laws and the ICRA name and logo are protected by the U.S. Trademark laws. http://www.icra.org/_en/legal/#notice

ICRA claims the right to sue someone who abuses its label.

Define the flow of money within the model, as it specifically applies to the certification and accreditation process (third party provider fees paid to the model owner for initial accreditation, third party continuing services/maintenance fees paid to the owner, identity issuer/relying party assessment fees paid to the third party auditor, identity issuer/relying party certification/accreditation fees paid to the owner).

"The ICRA labelling system is free for use by webmasters. Similarly, the ICRAfilter is free for use by parents and other concerned adults providing it is for their own personal use." http://www.icra.org/_en/legal/#notice ICRA is funded by sponsorships/donations.

ICRA appears to get some revenue from advertising on its web site and possibly advertising in the filter it distributes to parents.

An alternative implementation of this model would entail the sponsoring organization charging for use of its label and filter, and perhaps charging for automated and manual audits.

Define the dispute resolution process within the

model, as it specifically applies to all named participants, within the certification and accreditation process.

ICRA will contact web sites that appear to abuse its label and seek resolution. ICRA may sue if its label is abused. ICRA may also publicize information about an abusive web site and recommend that access to it be blocked by user filters.

Define the decision making processes each model owner utilizes to develop and deploy their model.

Web site administrators are urged to participate as a way to be responsible citizens and to help avoid liability and condemnation.

Parents adopt the ICRA filter to protect their children.

ICRA monitor's use of its label and seeks resolution when it discovers abuse.

Define the control/management processes each model owner utilizes to support their deployed model.

Web administrators act voluntarily.

ICRA monitors use of its label and acts when it sees abuse.

Define the length of time that a third party auditor accreditation and/or identity issuer/relying party assessment and/or certification/accreditation would be valid for.

Web administrators are expected to keep the label current at all times.

Model name: Product certification

Representative of the model: ICSA Labs, which certifies IT security products, such as firewalls and anti-virus software. See http://www.icsalabs.com

Summary: ICSA Labs sponsors industry consortia within various segments of IT security products. One such segment is firewalls and another is anti-virus software. Within each product segment, ICSA tests and certifies products.

Although ICSA sets the standards/criteria by which it tests products, each consortium influences those standards and criteria. http://www.icsalabs.com/html/communities/firewalls/index.shtml
Each consortium serves as a source of information and ideas about the latest threats and responses. In addition to the consortia, ICSA openly consults with experts and industry customers as it sets standards. http://www.icsalabs.com/html/certification/index.shtml

Products that achieve certification are permitted to bear the ICSA Labs seal. ICSA publishes on its web site lists of the products that are certified, together with highly detailed reports on the testing of each product, including strengths, weaknesses and unique issues.

Testing is an interactive process. Vendors are allowed to assist ICSA by patching products or changing configuration. All this assistance is noted in the testing reports.
http://www.icsalabs.com/html/communities/firewalls/faqs/index.shtml

Certification is not an event. It is an on-going process. ICSA continuously deploys each certified product on-site and expects the vendors to maintain the product as it would at a customer site. Any product that is certified can lose its certification at any time. In order to keep current with the latest IT attacks, ICSA regularly reviews and changes its testing criteria and can apply the criteria against certified products at any time. Vendors thus have constant incentive to upgrade their products.
http://www.icsalabs.com/html/library/DataSheets/Firewall_Data.pdf

ICSA uses a "black box" approach to testing. This means it devotes little effort to critiquing the engineering behind a product. Instead, it tests the product's performance. If the product performs to standard, then it is certified.

In addition to certifying products, ICSA sponsors surveys, buyer's guides and other materials to help educate customers of security products. http://www.icsalabs.com/html/communities/firewalls/index.shtml

Is the schema model based on in internal or third party certification process?
The model is purely third party certification. Testing is performed either by ICSA staff or by third parties authorized by ICSA.

Define the liability framework associated with each named participant within the model, specifically as it applies to the certification and accreditation process.

It does not appear that ICSA Labs has given much if any thought to liability. It openly publishes its certifications on its web site, with no disclaimers.

ICSA has probably never experienced any allegation of liability and has probably never sought counsel on the subject. ICSA could easily lower its exposure to product customers by publishing a disclaimer on its web site.

ICSA could also lower any exposure to vendors by contract with the vendors. ICSA does have a form of contract, but it simply focuses on an attestation by the vendor that it will continually provide all the information and support ICSA needs to perform its test.
http://www.icsalabs.com/html/communities/firewalls/certification/program/Checklist.rtf

ICSA does warn/educate its consortium members about antitrust liability. It publishes antitrust guidelines informing members they should not use the consortium to discuss prices or market allocation.
http://www.icsalabs.com/html/library/Antitrust.pdf

Vendors are liable to their customers according to the contracts between them.

Define the flow of money within the model, as it specifically applies to the certification and accreditation process (third party provider fees paid to the model owner for initial accreditation, third party continuing services/maintenance fees paid to the owner, identity issuer/relying party assessment fees paid to the third party auditor, identity issuer/relying party certification/accreditation fees

paid to the owner).

ICSA Labs charges vendors fees for testing and membership in the consortia. Customers can view certification/testing reports at no charge.

The parent company of ICSA Labs apparently gives access to product buyers' guides at no charge, though the parent probably tries to sell other products and services to customers.
https://www.trusecure.com/premium/login.shtml

Define the dispute resolution process within the model, as it specifically applies to all named participants, within the certification and accreditation process.
ICSA Labs urges vendors to be involved in the process of setting product standards. Then it urges vendors to patch or upgrade their products that fail the testing process. If a product is not performing to standard, ICSA communicates with the vendor's customer service people to see if they can remedy the problem.

Define the decision making processes each model owner utilizes to develop and deploy their model.

ICSA sets standards, conducts tests and publishes results. In setting standards seeks input from customers, experts and vendor consortia.

The only decision a vendor makes it whether it wants to participate.

The decision a customer makes it whether it wishes to assign weight to the results published by ICSA Labs.

Define the control/management processes each model owner utilizes to support their deployed model.

ICSA sets standards, conducts tests and publishes results. In setting standards seeks input from customers, experts and vendor consortia.

Define the length of time that a third party auditor accreditation and/or identity issuer/relying party assessment and/or certification/accreditation would be valid for.

ICSA Labs repeats the full testing process on an annual basis, but each product is subject to spot testing at any time. If a product fails spot testing and the vendor fails to remedy the problem within a short grace period, then the certification is revoked.
http://www.icsalabs.com/html/certification/index.shtml

Model name: Accreditation of an Institution

Representative of the model: Joint Commission on Accreditation of Healthcare Organizations - Hospital accreditation

Summary: This model accredits the staffing, resources and procedures within an institution, i.e. a hospital. The accreditation body is a private sector, industry association.

"An independent, not-for-profit organization, JCAHO is the nation's predominant standards-setting and accrediting body in health care. . . . JCAHO is governed by a 29-member Board of Commissioners that includes nurses, physicians, consumers, medical directors, administrators, providers, employers, a labor

representative, health plan leaders, quality experts, ethicists, a health insurance administrator and educators. . . . JCAHO's corporate members are the American College of Physicians-American Society of Internal Medicine, the American College of Surgeons, the American Dental Association, the American Hospital Association and the American Medical Association." http://www.jcaho.org/about+us/index.htm

A hospital is not required to be accredited, but accreditation helps a hospital with insurance, liability, winning of managed care contracts and so on. http://www.jcaho.org/about+us/index.htm

In most states, hospitals are licensed by government. JCAHO accreditation complements state licensure. It fulfills licensure requirements in many states, thus relieving the state of much of the burden of examination.

JCAHO publishes standards in consultation with experts and interest groups. JACHO provides interpretations about its standards. Then it surveys hospitals to determine whether they are meeting the standards. A survey results in a detailed report, including suggestions for improvement, which is kept private.

JCAHO publishes on its web site the accreditation status of a hospital (accredited, provisionally accredited, and so on), as well as a performance report, which "provides detailed information about an organization's performance and how it compares to similar organizations." http://www.jcaho.org/about+us/index.htm JCAHO will publicly place a hospital on "accreditation watch" status when JCAHO learns of a special event at a hospital that calls for attention.

In published performance reports, JCAHO will identify areas requiring improvement, and give hospitals a period of time to demonstrate improvement. JCAHO then revises the performance report to show the improvement whether the improvement was made.

Before a hospital is surveyed, it must announce to the public that a survey is planned so that members of the public can provide input. http://www.jcaho.org/htba/hospitals/survey+process/public+information.htm Through its web site, JCAHO solicits complaints about accredited hospitals. http://www.jcaho.org/quality+check/guides/hos.htm

The objective of accreditation is not merely for a hospital to pass the triennial survey. It is for the hospital to satisfy the standards all the time. A hospital is required to maintain records about its performance across time. http://www.jcaho.org/htba/hospitals/survey+process/preparing+for+survey.htm Surveyors look for evidence that the hospital maintains procedures and resources for sustained compliance.

JCAHO maintains an independent affiliate named Joint Commission Resources. JCR provides confidential advice and education to hospitals, but JCAHO and JCR keep a Chinese wall between themselves. They do not share information as to the accreditation status of a hospital or the delivery of advice from JCR. http://www.jcaho.org/about+us/index.htm

Is the schema model based on in internal or third party certification process?

JCAHO is a third-party accrediting body, and it employs its own examiners.

Define the liability framework associated with each named participant within the model, specifically as it applies to the certification and accreditation process.

JCAHO publishes a detailed policy on how it releases information (including certain information about performance and complaints) and which information it keeps confidential. The purpose of keeping some information confidential is to encourage candor on the part of surveyed hospitals. http://www.jcaho.org/lwapps/perfrep/infplcy.htm

In connection with the accreditation and performance reports that JCAHO publishes openly on its web site, there appear to be no disclaimers of liability. Evidently JCAHO has not sensed any exposure to liability to hospital customers reading report. JCAHO could easily publish a disclaimer that reduces potential liability.

Given that JCAHO publishes detailed policies on how it uses and discloses information, a hospital that participates in a survey implicitly agrees to those policies and cannot sue for defamation so long as the policies are followed.

Define the flow of money within the model, as it specifically applies to the certification and accreditation process (third party provider fees paid to the model owner for initial accreditation, third party continuing services/maintenance fees paid to the owner, identity issuer/relying party assessment fees paid to the third party auditor, identity issuer/relying party certification/accreditation fees paid to the owner).

A hospital pays a fee when JCAHO surveys it. The amount of fee varies depending on such factors as the size of the hospital.
http://www.jcaho.org/htba/hospitals/cost+of+survey.htm

Hospital customers do not pay JCAHO.

Define the dispute resolution process within the model, as it specifically applies to all named participants, within the certification and accreditation process.

When JCAHO cites a hospital for areas in which it can improve, the hospital is given time to show improvement.

Accreditation by JCAHO is a voluntary process. Revocation of accreditation is a blow to a hospital's reputation, but does not necessarily put the hospital out of business.

A revocation of state license could put a hospital out of business. Procedures for license and revocation vary from state to state, but normally state license law will provide an avenue for appeal if a state authority acts to revoke a license.

Define the decision making processes each model owner utilizes to develop and deploy their model.

JCAHO is a non-profit owned and controlled by leading members of the healthcare community. It sets standards based on community input. It communicates accreditation results by publication and by private consultation with subject hospitals.

State licensure of hospitals is normally government by a state regulatory agency.

Define the control/management processes each model owner utilizes to support their deployed model.

Hospitals are expected to set up internal teams to promote compliance with JCAHO standards. JCAHO, a third party industry association, then surveys hospitals for compliance. Apart from surveys, it also accepts and acts on complaints from the public.

Define the length of time that a third party auditor accreditation and/or identity issuer/relying party assessment and/or certification/accreditation would be valid for.

"To earn and maintain accreditation, an organization must undergo an on-site survey by a JCAHO survey team at least every three years." http://www.jcaho.org/about+us/index.htm

JCAHO also performs random, unannounced surveys.
http://www.jcaho.org/htba/hospitals/cost+of+survey.htm

Model name: Closed Contractual Club

Representative of the model: SWIFT

Summary:

"SWIFT is the industry-owned cooperative supplying secure, standardised messaging services and interface software to 7,600 financial institutions in 200 countries. The SWIFT community includes banks, broker/dealers and investment managers, as well as their market infrastructures in payments, securities, treasury and trade." http://www.swift.com/index.cfm?item_id=413225/25/2004

Historically, SWIFT's physical infrastructure was an X.25 network (in other words, an EDI Value-Added Network). Recently SWIFT launched a more versatile IP network called SWIFTNet.

Historically, SWIFT membership was generally limited to financial institutions regulated by national governments. SWIFT has many categories of membership, but generally membership required status as a regulated entity and in some cases approval/sponsorship by a committee representing the membership candidate's home country. See SWIFT corporate rules at http://www.swift.com/index.cfm?item_id=41961

Today, SWIFT has started to allow corporations to use SWIFTNet to communicate with one or more banks (but not with other corporations). In order to for a corporation to participate, it must be sponsored by a member bank. Gianfranco Tabasso, "SWIFTNet – The Next Revolution in International Cash Management?" www.treasury-management.com/Research/Byissues/03/jan03/Tabasso.pdf The sponsoring member bank is required under SWIFT Corporate Rule 2.3 to know and monitor the corporate participant. The member bank certifies to the SWIFT community the identity of the corporate participant. http://www.swift.com/index.cfm?item_id=41961

In this model, permission to participate is based more on reputation, prestige and sponsorship than on the satisfaction of particular financial, technical or security criteria. This model is relevant to the present study because private parties in an authentication network may be satisfied with one another (or at least with some special participants) so long as each participant is sufficiently large, has enough reputation at stake or is sponsored by a qualified party.

For example, the network might be supported at its core by several well-established trade associations (e.g., US Chamber of Commerce), and the reputation of each association may be sufficient to justify its membership regardless of financial or technical criteria. In effect, the associations could decide each can participate based on mutual consent. What is more, each core trade association may be permitted to sponsor participation by particular corporations using standards selected by the association. In the

alternative, an association might be permitted to sponsor only, say, publicly-traded corporations with market capitalizations of at least $2 billion.

The advantage of basing participation on reputation, recommendation, sponsorship and/or consent is that, in the proper environment, it is much more practical and efficient than requiring third-party audits and accreditation.

It may be possible that certain members of a network, based on reputation, recommendation or sponsorship, are expected to provide less in the way of audits or accreditation.

This model reminds us that rigid legal requirements and allocations of liability are not the only way to create an effective community among institutional peers.

Is the schema model based on in internal or third party certification process?

It is based on reputation, recommendation or sponsorship.

Define the liability framework associated with each named participant within the model, specifically as it applies to the certification and accreditation process.

Contracts govern the division of operational liability among the SWIFT network and its members. But those contracts do not cover the subject of liability for the admission, recommendation or sponsorship of an unqualified party into the SWIFT community. Although the SWIFT by-laws and corporate rules provide procedures for admitting new participants, including sponsorship, recommendation and vote-based consent, they do not formally assign liability to entities that make mistakes in sponsoring, recommending or voting for participants. Still, under the by-laws participants may be expelled for such general matters as an "act of negligence which may be prejudicial to the interest of the Company." SWIFT By-laws Article 13 d and General Terms and Conditions Clause 7.3. http://www.swift.com/index.cfm?item_id=7229

Define the flow of money within the model, as it specifically applies to the certification and accreditation process (third party provider fees paid to the model owner for initial accreditation, third party continuing services/maintenance fees paid to the owner, identity issuer/relying party assessment fees paid to the third party auditor, identity issuer/relying party certification/accreditation fees paid to the owner).

In order for a corporation to be sponsored by SWIFT member, the corporation will need to have a good relationship with the member. In practice, this means the corporation would have a banking relationship with the member substantial enough to justify the member going to the trouble, and risking its reputation, to sponsor the corporation.

Define the dispute resolution process within the model, as it specifically applies to all named participants, within the certification and accreditation process.

A member that sponsors a corporation is expected to have procedures for monitoring and presumably expelling the corporation if warranted.

The By-laws provide procedures for the board of directors to expel members with cause.

Define the decision making processes each model owner utilizes to develop and deploy their model.

Decision-making is a consultative process. Often, membership decisions are based on recommendations and input from industry representatives from a membership candidate's home country. Membership decisions are often based on votes and sponsorship.

Define the control/management processes each model owner utilizes to support their deployed model.

When a member sponsors a corporation, the member is responsible for monitoring the corporation and ensuring compliance with standards such as anti-money laundering laws. Shortcomings can lead to the withdrawal of sponsorship.

The SWIFT board of directors monitors the performance of members, and can expel members if cause is present.

Define the length of time that a third party auditor accreditation and/or identity issuer/relying party assessment and/or certification/accreditation would be valid for.

Monitoring occurs continually and expulsion can happen at any time.

/end/