ISSUES ANALYSIS BRIEF: SNAP-IN CONTRACTS ARCHITECTURE
MAY 25, 2004, EAP BRP Workgroup

Prepared by Daniel Greenwood, Esq.,

Background

At the last meeting, the BRP workgroup was presented with four potential ways to meet the goals and requirements of the EAP, while also respecting the emerging areas of consensus of workgroup members developed at prior meetings. Of them, there was a strong consensus for option 2, called the "snap-in" contracts approach. The basic elements of each option are described in Appendix 1, below. More relevant background is included, so as to document the decision making process, in Appendix 2.

Business Goals

It is useful to reiterate the most relevant goals of the EAP for the BRP, as reflected on the EAP web site and the majority of the presentations. The other goals are included in Appendix 2.

> *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.*

Description of "Snap-In" Contract Option

Each EAP Credential Service Provider (CSP) presents for pre-approval one or more standard Relying Party contracts to the EAP. The contract or contracts of the CSP are made available to any prospective Relying Party in advance of the Relying Party deciding whether to accept a credential from that CSP.

Each such agreement would in effect be a contract of adhesion ("take it or leave it" contract). The contracts can be presented in a standard format, for ease of review by prospective Relying Parties. There is an opportunity for give and take on the substance of the contracts as part of the approval process at the EAP level. For example, there may be opportunities to include aggregate pricing, public sector discounts or other benefits to Relying Parties as a result of attaining CSP services through EAP rather than direct contracting outside of the EAP circle of trust.

The contracting device, to avoid re-negotiating and executing bilateral contracts anew between each Relying Party and CSP participating in the system would be to have the terms of pre-approved contracts incorporated by reference into an overarching set of contractually enforceable rules. Under such a method, a Relying Party would need only execute one opt-in contract to come under the rules, and the rules would explicitly include reference to the contracting terms with each CSP, updated as they are approved, amended or removed from the EAP circle of trust. To avoid coming under any particular CSP set of contractual provisions, a Relying Party would need only avoid accepting a Credential issued by that CSP under the Rules.

At the last BRP call, there was desire expressed that this process of contract approval operate on a separate track from the more technical Certification and Accreditation process. The reason being certification by auditors or other objective assessors appeared ill suited to the very subjective and nuanced evaluations needed for approving service terms of a contract. Such evaluations implicate subtle judgements involving legal, business, strategy, and even socio-political dimensions. The reasoning was that an EAP body (such as a sub-committee of the Board of Directors, or a proportionally appointed or elected stakeholder committee, for example) would be better suited to make such evaluations, to interpret in an evolving manner any criteria for approval that are set, and to engage in the back and forth with applicant CSPs on the content

of their contracts as part of the approval process. Whether a CSP would engage in contracts approval before, during or after certification by an accredited assessor was not discussed.

Pro's of Snap-In Option

The key positive elements of this approach include:

1. It provides a way to achieve the "no additional bilateral contracts" requirement. With the modular architecture of option 2, no additional procurements, bids, negotiations and completely stand-alone contracts are needed.

2. It is achievable with current technology. Once rules are set and opt in contracts are finalized, simple reference to existing technical standards and practices will suffice.

3. It does not require all CSPs and Relying Parties to agree to a single set of provisions. With option 3, by contrast, presumably all key stakeholders would have to reach consensus on a single set of rules that would cover multiple parties from the start. Eventual convergence around a small or single set of provisions may emerge over time and can be reflected in the rules or as a default master contract.

4. It provides sufficiently comprehensive, actionable and salient information in advance to Relying Parties. Relying Parties will have an opportunity to select from among the recognized EAP CSPs with reference to all of the relevant information needed to join the respective circle of trust. In this way, the EAP becomes a connecting circle, joining other circles of trust in a meaningful and actionable manner.

5. It represents a low bar to entry (by not requiring agreement to single terms for all or negotiation of new bilaterals every time), and hence provides a simple way for CSPs and Relying Partiies to sign up, and rapidly scale up globally.

6. It provides a step toward option 3 (more comprehensive rules that do not leave out stakeholders) and does not preclude option 4 (automated contracting practices). It avoids having to resort to option 1 (jettisoning some requirements of EAP).

7. It is consistent with the desire for federated identity management by reflecting and supporting the circle of trust architecture. At no point would anybody be outside the circle, and the contract provisions assure they are all trusted.

Con's of Snap-In Option

Some key negative elements of Option 2 include the following:

1. It requires prior disclosure of contracts by Relying Parties. This represents a step in a process that will take time and require procedures.

2. It requires creating criteria to judge acceptability. There may be more than one opinion about what criteria should be set, and some criteria `could favor some CSPs or Relying Parties over others. This will take time and executive level attention of participating EAP stakeholders.

3. It requires somebody to judge acceptability of CSP contracts based upon the criteria set. This is a functional role that remains to be allocated, and will require creation of procedures.

4. It requires some due diligence by each Relying Party AFTER signing up for rules of the EAP. The Relying Parties would, presumably, need to become familiar with the terms of each contract associated with credentials it may seek to rely upon.

5. It creates some transactional drag for amendments to CSP contracts, given that amendments would presumably need to be accepted as well. However, any drag in the amendment process may not be greater than that which would happen when amending the same contract with any one of the very large Relying Parties, including the US Federal Government.

Matrix of Key Elements of Various Options

Option	Bilateral Contracts Negotiated?	New Technology?	Same Terms For All Parties?
Narrow Scope	Yes	No	No
Snap-In	No	No	No
Prescriptive Rules	No	No	Yes
Auto-eContracting (like P3P)	No (select set provisions)	Yes	No (but finite # of provisions)

The above matrix is an oversimplification for ease of comparison across the four options presented. The first column, "Bilateral Contracts Needed?" indicates whether the option meets the EAP goals and requirements that there be no need for additional negotiation and execution of a bilateral contracts between each CSP and Relying Party using an EAP solution. The second column, "New Technology"? indicates whether new technology is needed that is not yet generally commercially available and adopted by a significant market of users. A "no" in this column assumes the technology is at least as available and adopted as implementations of the Liberty Alliance or the Microsoft Passport services and specifications. The third column, "One Contract For Al Parties?" indicates whether a single set of contract terms and provisions are required for all parties. A yes means that, while there may be gradations of specificity or stringency of the terms, the same provisions at each level of proscriptiveness are in place for all CSPs and Relying Parties.

Open Questions (non-comprehensive and in no special order)

1. In view of a further week of consideration, and the above deeper analysis, is it still the will of the BRP Workgroup to focus efforts around this approach.

    a) Would it be preferable to narrow the scope (according to option 1), and simply publish a "model contract" which could be modified at will by each party, resulting in bilateral contracts by and between the parties? This was specifically suggested by one comment on option 2.

    b) Would it be preferable to pursue more prescriptive rules, as proposed in the third option?

2. What matters would be left to the rules and how would they fit into the whole?

    a) Would matters like intellectual property and licensing of the EAP trust mark be left to the rules? Would it make sense to include more detailed dispute resolution in the overarching rules, which would apply no matter which CSP or Relying Party presented? Would it makes sense to use the rules to create a reserve fund and decision making process for the internal absorption of some EAP risks (such as the Insurance Captive or other reserve explored in Appendix 2)?

    b) What would be the "order of precedence" between the EAP rules and the CSP contracts incorporated by reference into those rules? That is, in the event of a conflict, would the terms of the CSP contract win or would the other terms of the EAP rules control?

3. What specific matters would be the subject of certification by accredited assessors, and how would they fit with the matters left to the rules and incorporated contracts? Would there be overlap or gaps? Which matters are most efficiently and effectively allocated to each of these sources of authority?

APPENDIX 1: The Four Basic Options (excerpted)

1. Narrow the Scope: A system that works for the lowest assurance level and assumes no required additional contract. In other words, indicating that higher assurance levels (where the bilateral contract requirements arise more urgently) are out of scope, are simply out of scope (dealt with later or not). Alternatively, EAP could abandon the concept that a set of rules can or should replace bilateral agreements, and instead put forth a generic accreditation scheme that assumes every party also negotiates an individual contract.

2. "Snap In" Non-Standard Contracts of Adhesion by CSPs: Each Certified CSP presents for pre-approval a standard Relying Party contract as part of the Certification process (or, alternatively, after Certification, as part of opting into the EAP Rules). This contract is made available to any prospective Relying Party in advance of the Relying Party deciding whether to accept a credential. Each such agreement would in affect be a contract of adhesion ("take it or leave it" contract). It would be possible to present the materials in a standard format and possibly to negotiate through EAP certification processes somewhat more beneficial terms (aggregate pricing, public sector discounts, etc) than would be available outside of the EAP circle of trust. A variation of this method would be to incorporate by reference into the EAP Rules the terms of each pre-approved contract, avoiding the need for parties to individually accept each such contract each time it is presented.

3. Standard OpRules More Prescriptive At Higher Assurance Levels: An OpRules system with tiers, where use of Credentials at higher levels of assurance correlate to ever more prescriptive provisions of Operating Rules. This method assumes the relevant decision makers and counsel for each EAP stakeholder are prepared to negotiate conclusively on behalf of their organizations final terms that will be acceptable for use in place of the bilateral contracts otherwise required by each organization. A feature of forming this tighter knit circle of trust is ability to create a reserve fund to cover certain expenses, such as costs of disputes among parties or costs of credentials use.

4. Automatable Electronic MicroContracts: A system that includes "framework" provisions, selectable at time of opt in, and incorporates standard templates for the rest of legal agreements (like the P3P contracting model). Modular, in some sense, as the CSP would "snap in" its terms to the standard template, for ease of review and contracting processing. Such terms could be marked up in a dialect of XML (such as the OASIS/LegalXML emerging specification for eContracts) and Relying Parties could set authentication systems to accept certain combinations or particular terms and reject others in advance of being presented with any given credential and affiliated set of terms. This option relies upon technologies and standards that are relatively cutting edge and still emergent. As such, this method would require more discussion before being ripe for outlining and modeling and thus is not expanded below.

APPENDIX 2: Background Information

BUSINESS AND LEGAL RULES TERMS SHEET VERSION 4.0, MAY 18, 2004
For the EAP BRP Workgroup

Presented by Daniel Greenwood, Esq., Semivirtual@yahoo.com or 857-498-0962.

Abstract: This iteration of the Terms Sheet presents four possible architectures to meet the goals of the EAP consist with the consensus reached at the prior meeting. The two areas of consensus were that the BRP should develop rules and practices that are not so prescriptive they exclude important credential providers and that assume a model whereby accreditation/certification operates along with a set of legal/business rules applicable to parties using EAP credentials. The EAP goal most relevant to the BRP is to replace bilateral agreements currently required for use of third party credentials. It is envisioned that this goal can be achieved by replacing the bilateral agreements with a set of Rules applicable to parties using credentials under an EAP umbrella. The BRP Workgroup is tasked with creating the Business Rules and Practices.

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.

"Rules of Engagement"

The third goal, drafting "rules of engagement" to replace bilateral agreements, presents the task most relevant to the BRP. There is no known way to achieve this goal solely by use of a Trust Mark or other generic certification and accreditation system. The key issue is that a Trust Mark (or other certification issued to a CSP upon by an accredited organization based upon generic criteria) does not address various factors generally required by relying parties and CSPs prior to allowing reliance upon a credential. If it were assumed that EAP credentials required little or no assurance by the relying party, it would be possible to develop a meaningful Trust Mark based solely upon generic, non-legal and business level factors. Such non-legal or business level certification criteria may include matters like technical specifications used, physical and network security, identity proofing at time of credentialing, etc. However, such generic certification at multiple levels of assurance, is not capable of addressing the legal and business issues currently negotiated bilaterally. These issues include liability for the underlying transaction, payment to the credential service provider, use of intellectual property (including business trademarks) of each party, indemnities, service level agreements, and several other issues. Nor is it realistic to assume a widely usable system meeting the stated goals of the EAP absent direct treatment of these types of issues.

While it is possible to achieve the goal through use of a contractual and comprehensive set of overarching rules, creation of such a system is currently deemed out of scope of the EAP. It is desirable to avoid creating a system that is so comprehensive and detailed it would exclude

existing and relevant credential service providers that would otherwise participate in an EAP-enabled system. It is also desirable to avoid developing a set of rules that is overly complex and prescriptive at the outset of the EAP before much experience with the practical and technical aspects of such an undertaking has emerged. Rather, a more tiered and phased approach was desired at the last BRP workgroup call.

Four Possible Approaches to Solve the Problem: Overview

The four possible approaches are to 1. Narrow the goals of the EAP, or 2. Create a system whereby each accredited/certified CSP and Relying Party contract are collected in advance, put into standard formats, and incorporated by reference into a single opt-in master EAP contract, or 3. Negotiate a single contractual rule set with all the key CSPs and Relying Parties in advance whereby each agrees to accept the rules in place of its own contracts and where higher levels of assurance carry much more prescriptive, detailed and comprehensive terms, or 4. Develop a large library of standard applicable contract provisions that can be presented and parsed electronically, similar to P3P privacy preferences agreed between merchants and consumers.

Four Possible Approaches to Solve the Problem: Abstracts

1. Narrow the Scope: A system that works for the lowest assurance level and assumes no required additional contract. In other words, indicating that higher assurance levels (where the bilateral contract requirements arise more urgently) are out of scope, are simply out of scope (dealt with later or not). Alternatively, EAP could abandon the concept that a set of rules can or should replace bilateral agreements, and instead put forth a generic accreditation scheme that assumes every party also negotiates an individual contract.

2. "Snap In" Non-Standard Contracts of Adhesion by CSPs: Each Certified CSP presents for pre-approval a standard Relying Party contract as part of the Certification process (or, alternatively, after Certification, as part of opting into the EAP Rules). This contract is made available to any prospective Relying Party in advance of the Relying Party deciding whether to accept a credential. Each such agreement would in affect be a contract of adhesion ("take it or leave it" contract). It would be possible to present the materials in a standard format and possibly to negotiate through EAP certification processes somewhat more beneficial terms (aggregate pricing, public sector discounts, etc) than would be available outside of the EAP circle of trust. A variation of this method would be to incorporate by reference into the EAP Rules the terms of each pre-approved contract, avoiding the need for parties to individually accept each such contract each time it is presented.

3. Standard OpRules More Prescriptive At Higher Assurance Levels: An OpRules system with tiers, where use of Credentials at higher levels of assurance correlate to ever more prescriptive provisions of Operating Rules. This method assumes the relevant decision makers and counsel for each EAP stakeholder are prepared to negotiate conclusively on behalf of their organizations final terms that will be acceptable for use in place of the bilateral contracts otherwise required by each organization. A feature of forming this tighter knit circle of trust is ability to create a reserve fund to cover certain expenses, such as costs of disputes among parties or costs of credentials use.

4. Automatable Electronic MicroContracts: A system that includes "framework" provisions, selectable at time of opt in, and incorporates standard templates for the rest of legal agreements (like the P3P contracting model). Modular, in some sense, as the CSP would "snap in" its terms to the standard template, for ease of review and contracting processing. Such terms could be marked up in a dialect of XML (such as the OASIS/LegalXML emerging specification for eContracts) and Relying Parties could set authentication systems to accept certain combinations or particular terms and reject others in advance of being presented with any given credential and affiliated set of terms. This option relies upon technologies and standards that are relatively

cutting edge and still emergent. As such, this method would require more discussion before being ripe for outlining and modeling and thus is not expanded below.

Terms Sheet Outline Tracking Each Method

The following drafts contain only the most relevant and important terms and the substance of those terms serves only as placeholder text at this time. It is presumed that legal counsel and executive management of key EAP members would review, negotiate and agree upon final language in advance of finalization. Further, it is assumed that Membership agreements other than these rules and contracts would cover liability or other obligations and rights of Members of the EAP, including duties to pay dues and disclose intellectual property rights triggered by contributions to EAP standards.

Generic Terms (Expected under any of the 4 methods).

Scope:

These Rules govern the use, acceptance and validation of identity credentials issued by an EAP Certified Credential Service Provider (CSP) instantiated in a token bearing the branding of the EAP (EAP credential). These Rules apply to each Relying Party and CSP who issue, accept and/or validate an EAP Credential.

Eligibility and Opt In Contracts:

Relying Parties and CSPs: Each Relying Party and CSP must agree to be bound by these Rules by accepting the appropriate Opt In Contract [NOTE: include link here to then current official Opt In Contract for each party]. Before becoming eligible to Opt In to these EAP Rules, a Relying Party must first be Certified by an EAP Accredited Certifier to issue EAP Credentials at one or more levels of assurance. Before becoming eligible to accept, rely upon or validate an EAP Credential, a Relying Party must first accept the Relying Party Opt In Contract.

End Users: Each CSP agrees that every end-user identified by an EAP Credential and presenting it for identity authentication to a Relying Party has accepted an EAP End User Opt In Agreement [NOTE: Include link] prior to issuing an EAP Credential. Each Relying Party agrees that every end-user identified by an EAP Credential and presenting it for identity authentication by that Relying Party has accepted an EAP End User Identity Linking Agreement before relying upon and/or linking the EAP Identity to a Relying Party identifier for that end user.

Intellectual Property

EAP Trust Mark on Tokens, Web Sites and Other Materials: [Include authorized uses and prohibited uses here, as well as infringement and licensing terms].

Method 2 (Relevant Contracts Incorporated by Reference)

Pre-Approval of EAP Party Contracts Requiring Additional Assent

Pre-Approval of Contracts: Each CSP must either

1. Warrant that no additional contract is required in order for an EAP Credential to be used, relied upon and/or validated by an EAP Relying Party, other than the EAP Opt In Agreement and these EAP Rules, or

2. Present to [either the Accredited Certifier as part of Certification or to the EAP as part of Opt In to the Rules] each applicable contract at each assurance level necessary for any EAP Relying

Party to accept, rely upon and/or validate an EAP Credential issued by that CSP for prior approval.

CSP Application for Pre-Approval of Contracts: To be accepted for pre-approval, each such contracts must meet the minimum requirements of the EAP Certification requirements and also these EAP Rules, as applicable to the level of assurance for which the EAP credential is approved. A CSP may have one or more contracts accepted and one or more other contracts rejected. In the event one or more contracts are not accepted, the CSP applying for acceptance will be delivered the reasons for rejection and an opportunity to revise the contracts and re-submit them accordingly.

Relying Party Access to Pre-Approved Contracts: Each pre-approved contract of an EAP CSP shall be available for inspection by every EAP Relying Party at any time. [NOTE: Granting each EAP Relying Party authorization to an online access-controlled repository of pre-approved contracts for browsing and review would be an easy method.].

Manifestation of Assent to Pre-Approved Contracts: At the time of Validation of an EAP Credential by a Relying Party, the applicable pre-approved contract or a link to same shall automatically be presented to the Relying Party. The Relying Party shall not be permitted to validate the EAP Credential unless it accepts the applicable agreement. [Note: These Rules could list of affirmative acts constituting acceptance, such as clicking "ok" or sending back an automated message according to a unique and specified syntax and content by the Relying Party authentication system]. The validation process must permit the Relying Party to accept the pre-approved contract for that session and reliance usage only, or for a period of time during which the EAP Credential shall be available for multiple or unlimited acceptance, reliance and validation by the Relying Party. Any terms, including transaction fees, payments per use or period of time or other formula and other applicable terms must be presented clearly in the pre-approved contract.

Amendment: A CSP may apply to amend terms of pre-approved contracts at any time and may opt to either 1. Have the existing unamended pre-approved contract remain in place while the application for amendment is being processed or 2. Terminate future use of the pre-approved contract while the application for amendment is being processes, resulting in a removal of the EAP Credential for which that contract is required form the EAP Credential system until and unless a replacement contract is approved.

INCORPORATION BY REFERENCE VARIATION OF METHOD TWO

Incorporation by Reference: Upon being accepted [alt 1: "as part of CSP Certification" or alt 2 "as part of Opting into these EAP Rules by a Certified CSP"] a pre-approved contract shall be incorporated by reference into these EAP Rules and applicable to any EAP Relying Party that accepts, relies upon and/or validates an EAP Credential to which such contract applies.

Contract Number: Each contract accepted for pre-approval shall be identified by a unique number, referenced in the EAP Rules. The token in which each EAP Credential is instantiated shall not be capable of validation without reference to the contract number. (Alt: Require that any acceptance, reliance and/or validation somehow require reference to the contract number, not solely the validation process).

Voluntary Acceptance, Contract by Contract: Reliance upon an EAP by an EAP Relying Party shall constitute acceptance of the respective pre-approved contract. No EAP Relying Party is obligated to accept, rely upon and/or validate an EAP Credential. An EAP Relying Party may choose not to rely upon an EAP Credential and thereby avoid acceptance of the section of the EAP Rules referencing that contract. Acceptance of one EAP Credential and related pre-approved contract incorporated by reference does not imply or require acceptance of any other EAP Credential or any other pre-approved contract.

METHOD 3: (Rules More Prescriptive At Higher Assurance Levels)

Note: The following terms are presented as examples only, and derive from Yahoo! and MSN Passport publicly available web-based contracts applicable to third party use of credential issued by those CSPs. For more, but only partial, detail, see http://ecitizen.mit.edu/EAP/Yahoo-Passport/ Other potential sources of applicable terms can be found at http://ecitizen.mit.edu/EAP/RulesExamples/ (compilation of publicly accessible web-based Operating Rules). It is envisioned that this approach would contain several tiers, each becoming more detailed and comprehensive to address respectively higher levels of assurance by Relying Parties. The current Federal levels of assurance are: Level 1: Little or no confidence in the asserted identity's validity, Level 2: Some confidence in the asserted identity's validity, Level 3: High confidence in the asserted identity's validity, and Level 4: Very high confidence in the asserted identity's validity.]

Support

Lower Level "The EAP CSP will make reasonable efforts to maintain a support service for EAP Relying Parties for the purpose of receiving inquiries, complaints or urgent requests involving use or validation of an EAP Credential issued by that CSP. The EAP CSP reserves the right to establish limitations on the extent of any support provided for the Credential Service, and the hours at which it is available."

Higher Level "The EAP CSP will maintain a 24/7 call center for use by any EAP Relying Party in relation to the use of validation of EAP Credentials issued by that CSP. The CSP call center shall publish its escalation policy for review by any EAP Relying Party, detailing how complaints or urgent requests are taken in, assigned priority, and the conditions under which they are escalated to an executive decision maker within the CSP. The CSP call center shall be accessible by telephone and also by e-mail, and shall specify response times for each newly ticketed request for service no less than 2 hours from the time of intake."

Payment

Lowest Level: [Alt 1. No Fee] "There shall be no fee to Relying Parties for use of, reliance upon or validation of an EAP Credential that have been certified at Level One, the lowest level of assurance. Nothing in this section prohibits the Relying Party and CSP from agreeing upon the terms of other value-added services or products available from the CSP which may entail a fee. [Alt 2. Nominal Fee] "For each EAP Credential an EAP Relying Party accepts, relies upon and/or validates, the Relying Party shall pay a one time fee of $X to the issuing CSP].

Higher Levels [Alt 1. Based upon Passport] There are two fees for licensing EAP Credential usage: a periodic compliance testing fee of US$1,500 per URL where the Credential will be re-used by an EAP Relying Party and a yearly provisioning fee of US$10,000 per EAP Relying Party. The provisioning fee is charged on a per-Relying Party basis and can be applied to multiple URLs. For example, if your company relies upon EAP Credentials on three distinct URLs, you would pay one yearly fee plus the periodic compliance testing fee for each of the three URLs. This entitles your company to unlimited volume use of the EAP Credential service at those URLs."

[Alt 2. Based upon idea of an "Insurance Captive" for authentication developed by MIT's E-Commerce Architecture Program, at http://actuarinet.mit.edu]. "Each Relying Party shall pay $X USD into the Service and Risk Pool of the EAP annually in return for use of, reliance upon and validate of EAP Credentials. From that fund, a reserve account to mitigate or absorb the risk of loss events involving the EAP of no less than $$ (dollar amount, percentage or other formula) shall be maintained, and the remainder shall be distributed on a quarterly basis to every EAP CSP up to $$ (amount, pro-rata based on validations of credentials, or other formula), and any

excess amounts resulting in a proportional decrease of the fee paid in the subsequent year. " [NOTE: A variation on this alternative could include all parties, CSPs, and Relying Parties, and potentially others, all paying into the risk pool. Another variation could have this pool used only to absorb loss events and not also as a payment mechanism for CSPs. A final variation could have the CSPs be the only party paying into the pool and presumably passing the costs back to the end-users.]

Privacy Policy:

[Alt 1. Based upon Yahoo! Merchant Agreement] You agree (a) to post a privacy policy in Your site that, at a minimum, discloses any and all uses of personal information that You collect from users; (b) to include in Your privacy policy a paragraph provided or approved by the CSP that describes the CSPs collection and use of Credentialed User's information, (c) to provide a hypertext link to Your privacy policy on the home page of Your referring and on all pages where You collect personal information from users, including but not limited to all check out pages; and (d) to use personal information only as expressly permitted by Your privacy policy.

[Alt 2. Based upon MSN Passport, As paraphrased in Passport Review Guide]

The information stored in a EAP Credential account is not shared with EAP participating sites or services unless the user explicitly chooses to provide it by clicking the EAP sign in button.

By clicking on the sign in logo at your site or service, the user consents to have his or her selected EAP Credential profile information delivered to you. With the user's consent, within the guidelines of your own privacy statement, consistent with the Opt In agreement signed between EAP and your organization, and consistent with any privacy coalition program in which you participate (e.g. TRUSTe or BBBonline), you can then store and use the information you receive from the user's EAP Credential profile in exactly the same way you could have used this information if you had collected the information yourself. You can also use the EAPUID as the unique key identifier for the EAP Credemtialed user inside your own database.

However, by signing the EAP Opt In contract you agree to some specific restrictions in your use of EAP Credential data. These include:

- You can use EAP profile information only to deliver the products and services requested by users.
- You cannot use EAP profile information to contact users for any purpose without obtaining the users' prior consent.
- You cannot assign, transfer, share, transmit, or publicly disclose EAP profile information—or any identifiable information gathered from Passport profile information—to any third party without the user's consent.
    - The only exception to this last requirement is when you need to transmit EAP Credential information to third parties in order to deliver goods and services requested by the Passport user (for example, if the participating site sends some of its business, such as shipping services, to an outside provider). In this case:
        - If the third party is another EAP participating site, you may transmit the EAPUID.
        - If the third party is not a participating organization, you may transmit profile data to third parties, with the following restrictions:
            - The data may only be sent for the purpose of allowing such third parties to participate in the delivery or fulfillment of a product or service requested by the user.

        - Only the amount of profile data that is reasonably necessary for such third parties to receive in order to deliver the product or service requested by the user may be sent.
        - Each third party that receives such data from you must have agreed in advance of receiving such information to:
            - Use such data only for the purpose of delivering the product or service requested by the user; and
            - Respect terms no less restrictive than these listed here.
- You agree to post privacy policies on your site and adhere to legal privacy requirements and industry standards. EAP also now calls for you to comply with the Platform for Privacy Preferences Project ("P3P") specifications set by the World Wide Web Consortium ("W3C"). This means that you expose your privacy statement in the form of an XML document that conforms to the W3C-P3P specifications. You also post a compact statement describing their use of cookies in the form of a mini-header that conforms to the W3C-P3P specifications.
    - These documents and headers, in conjunction with the new Internet Explorer 6 support of P3P specifications, enable users to more easily understand a site's privacy statement and cookie usage. They also make it easier for users to define their default preferences for managing cookies.

Dispute Resolution

[Note: The following examples come from sources other than Yahoo! and MSN Passport]

Low Level of Assurance: [Derived from the MultiState Emall Operating Rules, available at: http://ecitizen.mit.edu/EAP/RulesExamples/EMALL/oprules-v2.htm] Disputes between a CSP and a Relying Party regarding use of, reliance upon or validation of an EAP Credential, shall be governed according to the terms and conditions contained within the underlying contract governing the transactions or other interactions engaged in by those parties for which EAP Credentials were used to authenticate one of the parties. Disputes arising out of or related to the application of these Operating Rules and related Opt In Agreements shall be resolved in accordance with the provisions of these Operating Rules and related agreements, and by agreement between the parties, where possible, through direct negotiation or, if appropriate, through voluntary mediation by a mutually agreed upon Mediator. In the event that parties are unable to reach agreement directly or through the use of mediation or other voluntary methods of Alternative Dispute Resolution, then, to the extent permitted by law and relevant regulation, all such disputes shall be subject to binding arbitration by a a mutually agreed upon arbitrator of the American Arbitration Association. The costs of any form of Alternative Dispute Resolution shall be paid equally by the disputants or as otherwise agreed by the parties."

Higher Level of Assurance:

[Alt 1. Detailed EBT Model] See Chapter 8 of the QUEST Operating Rules governing use of the Electronic Benefits Transfer Council, available on the web or at: http://ecitizen.mit.edu/EAP/RulesExamples/QUEST/1.4_May_2002.pdf

[Alt 2. Risk Pool Approach proposed by MIT E-Commerce Architecture Program, at http://actuarinet.mit.edu] [Note, this approach works with Payment provision Alt 2 for the higher level of assurance, and is broadly consistent with the practices of Insurance Captives which self-insure across enterprises in a similar risk pool and also with the Visa approach to reserve funds for internal allocation to cover certain limited disputed costs or other losses among parties to that system.]

Disputes involving liability for money damages between EAP CSPs and EAP Relying Parties shall, in the first instance, be referred to the EAP Executive Council [by whatever name it is called] for non-binding determination [query - shall we give end-users of EAP Credentials standing to raise disputes as well?]
. The Executive Council may opt to apply informal investigative inquiries, formal mediation or formal arbitration or any other method it deems appropriate to develop a proposed resolution to the dispute. The Executive Council is authorized to propose any settlement terms, consistent with these EAP Rules and Opt In Agreements, and may include an offer to one or more disputants of direct monetary compensation to be disbursed from the EAP Reserve Pool up to [include limits here, based on hard ceiling, percentage or other formula].

All parties agree to refer disputes not capable of voluntary resolution by the parties through negotiation or mediation to an Arbitrator for binding decision. The judgment of the arbitrator may be entered by any court having jurisdiction. [See the EBT Model above for further detail on potential additional arbitration provisions]. The arbitrator may hold one or more parties jointly and severally liable for damages arising out of or related to any dispute presented. To the extent no party is deemed liable, the arbitrator may allocate monies from the Reserve Pool of the EAP up to [$$ amount, percentage or other formula] and may hold one or more parties to the dispute liable for the remaining damages, if any.

The Executive Council shall refer all disputes, including the final settlement arrangements, to a Risk Management Committee [by whatever name it goes in the final documents] to analyze and report back to the EAP recommendations to avoid, mitigate, transfer or otherwise address the cause of the dispute. These recommendations may include changes to these Rules or Opt In Contracts, changes to the practices governing contributions to and disbursement from the EAP Reserve Pool.

APPENDIX 2, Continued

BUSINESS AND LEGAL RULES IN TERMS SHEET: ALTERNATIVES FOR THE BRP WORK GROUP

Draft, May 11, 2004, by Daniel Greenwood, Esq., Semivirtual@yahoo.com or 857-498-0962.

Abstract: The following 2 paragraphs and 3 sets of alternatives frame the issues presented in this week's iteration of the "terms sheet" (business/legal rules for EAP): A. Do the rules cover underlying transaction risk, if not how is it handled, B. Is the system "open" or "closed", C. What is relation between Accreditation and these Rules? This memo and the Terms Sheet draft present closed, open a hybrid alternatives.

In federated "circles of trust" systems, Relying Parties and credential providers are all bound to each other under a contractual scheme defining rights, obligations, liability and other relevant terms. The EAP and federal use cases all assume a federated system in which credentials issued for one purpose (such as to a customer or employee) will be available for federal re-use for other transactions with potentially very different legal and business implications. Legal issues include liability for underlying transactions (as distinct from liability for mis-identification), use of intellectual property (such as trademarks or service marks of Credential Service Providers (CSPs) or Relying Parties). Business issues potentially include payment or other value from the Relying Party to the CSP in return for right to use credential and share customer and whether a CSP has the ability to limit which Relying Parties may use its issued credentials (e.g. whether it may prevent competitors from sharing customers or may define service level expectations, etc). These types of issues would be resolved and recorded through the process of contracting between the CSP and Relying Party when they created or joined a federation.

It has been stated that, ideally, EAP can result in a system whereby a large Relying Party, such as the U.S. Federal Government, need not negotiate a completely new contract for each CSP. To architect such a system, many business and legal issues would have to be addressed by the EAP contribution (either through the Accreditation process, through new sets of contractual business and legal rules applicable to all parties issuing or using EAP credentials, or otherwise). It is possible to imagine an EAP system whereby a very reduced number of large Relying Party contracts are necessary, perhaps in the order of the number of credit card industry contracts or mobile phone service provider contracts such parties now execute. Finally, it is possible that a large Relying Party could use an EAP Accreditation and Business/Legal Rule set as a type of "procurement schedule", whereby any CSP who is on an EAP list has proven reliable and stable enough to warrant a short standard agreement, such as a quoted price for a "scope of work", without the need for a full RFP, bid process and soup to nuts negotiation of all business and legal terms.

Revision of the Business/Legal Terms Sheet of the BRP requires further clarity on the following topics:

1. Scope of Business Rules:

Alternative A: Credit Card/ATM Model

The business rules and processes of the EAP follow the credit card industry model of a contractual multi-lateral rule set, defining all the relevant business and legal matters of the parties. Example: a "Visa" and "Cirrus" brands on a credit/ATM card reflect membership in a global, interoperable, membership system of issuers and relying parties (and others) who entered into contracts defining how each pays for services form the others, liability for underlying transactions, and other business and legal terms tailored to the transactions).

Alternative B: Trust Mark Model

The business rules and processes of the EAP follow the trust mark model of an accredited set of practices by the CSP, and assume each CSP and Relying Party will also need to negotiate a contract defining the relevant business and legal terms enabling transactions with credential holders. Example: A privacy seal or BBB seal, while conveying information relevant to "trust" decision, are not sufficient without other contracts or business context to support even small amounts of reliance).

2. Applicability of "Federation" and "Circle of Trust" Concepts to EAP

Alternative A: Closed Communities

EAP is a closed, membership based contractual circle of trust. The word "circle" in circle of trust means there is a boundary condition, and only parties who are "inside" the circle may participate. The word "trust" in "circle of trust" means the relevant enforceable terms structuring the business and legal relationships of all the parties inside the circle are sufficient to manage risk and assure predictable outcomes for disputes regarding the substantive transactions between parties. Federations are circles of trust almost always bounded by specific contracts (bi-lateral or multi-lateral) covering membership and delineating risk allocation for the underlying activities in the circle.

Alternative B: Open-PKI Model (Applied Technology Neutrally to Any Authentication Method)

EAP follows an Open-PKI Model, assuming an EAP credential would be like a Passport, used by potentially any relying party who chooses to trust the issuer, and can be used for virtually any purpose, with no permission or agreement from the issuer. There would be some standards that relate primarily to information field syntax, interoperability and naming conventions, but no limit on participation by any Relying Party (i.e.: no "circle") and would leave to other contracts, laws or agreements the determination of business and legal issues of the parties related to their underlying transactions and other activities.

Alternative C: Shortcut to Formation of Closed Communities, Built Upon EAP Foundation

EAP provides pre-vetting of various large and generally reliable (i.e.: deep pockets, sophisticated infrastructure, institutional commitment, etc) CSPs, and reduces the need for additional due diligence or contracting by prospective Relying Parties. The process of CSP/Relying Party match-making could be facilitated by EAP establishing such matters as the pool of Credential Holders (e.g. all AOL account holders, all Fleet account holders, all Sprint account holders, etc), the level of Assurance of the credential, the type and amount of insurance, and one or more standard contracts the CSP will accept from any potential Relying Party. Such "standard contracts" may require CSP giving a price, service quality and/or delay quote in response to a service request, and may permit the CSP to refuse to grant service under some circumstances. Depending upon the specific transactions sought, in some cases, Relying Parties and CSPs may choose to negotiate more precise or far reaching terms (such as co-branding details, joint advertising of the federated relationship, revenue-sharing, opening new lines of business, etc).

3. Relationship Between Accreditation of a CSP and the Business Rules and Processes

Alternative A: Accreditation is Eligibility for Becoming a Party to EAP Business/Legal Rules

Accreditation follows the model of certifying that a given party has proven eligible for membership in a closed EAP federation, or federation of federations (such as in alternative 2.B.) Example: Before certain large insurance companies will write a policy for particular types of so-called "cyber insurance" (e.g. covering lost business resulting from problems with web or other Internet usage), the applicant must pay for and undergo a detailed audit and information security review. A satisfactory certification that relevant practices, technology and agreements are in place must be achieved for eligibility to sign an insurance contract, opting into the contractual risk sharing community (and setting the premiums for that applicant).

Alternative B: Business Rules are a Factor Considered in Accreditation

Accreditation is the final step and conveys that the accredited party is certified to have in place business rules and practices that are generically sound. Example: A Certification Authority has a Certification Practice Statement and other agreements and policies and practices that are accredited to meet certain generic standards. This case assumes approaches like those in 1.B. and 2.B.

Alternative C: Business Rules and Accreditation Supplement Each Other

Accreditation address certain technical aspects of Credential issuance and maintenance, relevant to Relying Parties (such as the practices necessary to establish identity proofing measures, token strength and security of token delivery) while Business/Legal Rules of EAP address other aspects relevant to both Credential Providers and Relying Parties wishing to "do business". In this case, the Business/Legal rules could address the same types of matters contained in contracts underlying approaches in 1.A, 2.A and 3.A. However, the Accreditation could be relied upon in an open system whether or not the Relying Parties were

signatories to the Business/Legal Rules. However, applying some or all of the EAP rules, in this "supplementary" scenario, could shortcut or eliminate the negotiation and contracting steps otherwise probably necessary between Credential Providers and Relying Parties.

Terms Sheet Draft 3.0

Terms Sheet
Draft 3.0
May 11, 2004

1. Title of Document, Definitions and Scope.

[NOTE: A basic scope question is: Are EAP these rules and accreditation the only business and legal connection between a Credential Provider and a Relying Party such as the US Federal Government? If so, then it remains to be determined how underlying risk and liability for the transactions and information transmitted will be addressed. Other possibilities include:
* EAP Rules and Accreditation for Generic Identity Issues PLUS Contracts for Specific Business Issues. Example: The credit card model, where the federal government maintains a small number of independently negotiated contracts giving access to each major industry service provider with somewhat different legal terms, payment rates, etc, and a general set of policies applying to all credit card processing transactions government-wide.
* EAP Rules and Accreditation Address Both Generic Industry/Party Neutral Issues and Business/Risk Issues Arising from Underlying Transactions. Example: The Electronic Benefit Transfer Council Operating Rules and Opt-In Contracts.
* EAP Rules and Accreditation Address Generic Identity Issues, PLUS Modular Sections of Rules for Approved Pre-Existing Agreements by Participating Federated Identity Communities. This possibility could track alternatives 2.C and 3.C in the May 11, 2004 document " Business and Legal Rules in Terms Sheet: Some Alternatives for BRP Work Group".]

2. Roles and Functions

[NOTE: The following roles have been derived from EAP documents and meeting notes.]

2.1 Credential Service Provider

[NOTE: In order to operate under these rules, must a CSP be accredited first? If a CSP is accredited, must it also be recognized under the rules, or will/should it be necessary for the CSP to: 1. Sign an Opt-In Contract agreeing to the Rules, and/or 2. Become a Dues Paying Member of the EAP, and/or 3. Have Any Another Contract in Place With Relying Parties Addressing Industry-Specific, Transaction-Specific or Party-Specific Liability or Business Issues, and/or Other Requirements?]

2.2 Credential Holder (AKA User, Customer, Employee, Citizen)

[NOTE: This section would address: Minimum requirements for opt-in language, privacy disclosures, other rights or responsibilities such as maintaining security or getting/sending notices?]

2.3 Relying Parties

[NOTE: There remains a question as to whether the same rules and processes can and should apply to federal government external relying parties (the "C2G" scenario of the BRP WG) as will apply to private businesses. If the same rules are to apply, then all relying parties may be capable of treatment under one section.]

2.3.1 United States Government

2.3.2 Relying Party, Private Business

2.3.3 Relying Party, Other Credentialed Users

2.4 EAP Executive Committee

[NOTE: If there is to be an EAP decision making executive with authority over the rights and duties of other parties assuming roles within an EAP system, it would be consistent to identify that EAP executive in this section. The scope of authority over other parties should be identified here.]

[NOTE: There may be other roles, such as Accrediting Party, Auditor, Other Relying Parties, etc. The number and division of roles remains to be discussed by the BRP.]

3. EAP Membership

[NOTE: It remains to be determined whether EAP shall refer to CSPs and Relying Parties as "Members" or if the term Member shall only apply to a small set of representative parties playing a governance role and paying dues to have say over EAP rules. If the former, then this would be an appropriate section to deal with how a party becomes a member, how they are expelled, etc. If the latter, then this section can be left to the governance document or charter.]

3.1 Membership Eligibility, Rights and Duties of Members

3.2 Expulsion of Members

4. Dispute Resolution

[NOTE: KEY QUESTION: Shall dispute resolution - and the scope of EAP rules in general - deal with underlying transaction risk or simply deal with the narrow area of identity accuracy risk? See Liability note in section 5 of this document for further detail on option.]

4.1 Problem Reporting and Handling

4.2 Internal Problem Resolution

[NOTE: It may be appropriate to include role of EAP Executive arm in addressing determining interpretation of rules where Members or other contractual parties disagree, perhaps A. carving out a series of rules in the domain of the Executive to apply and other rules left to dispute resolution, or B. allowing the Executive to attempt to settle the disagreement on a voluntary internal basis, but allowing any unsatisfied party to seek resource externally through ADR.]

4.3 External Alternative Dispute Resolution

4.3.1 Mediation

[Note: It may be advisable to require or promote non-binding mediation by a neutral third party to attempt to resolve disputes among EAP system parties amicably before escalating to arbitration]

4.3.2 Arbitration

[NOTE: Issues include: how arbitrator is chosen, discovery and other process issues, whether there is a scope (monetary or otherwise) constraining possible awards, the binding nature of the arbitration, and the extent to which information from judgments and proceedings may factor into risk management or other evolution of EAP processes.

5. Liability

[Note: Key Question is how underlying transactional liability will be addressed by parties using EAP offerings. If such liability is not to be addressed by EAP, then it may be necessary for parties using EAP offerings to also negotiate and execute a bi-lateral or additional multi-lateral contract for every other party or circle of trust within the EAP. ***Example:*** *Company A (an online travel service) authenticates an individual via the Liberty spec. The individual proceeds to move to Company B (an online stock trading service) and explicitly links the accounts (federated SSO) via the Liberty spec. Said individual then attempts to sell a stock holding that is *dropping rapidly. For some reason, the authentication that Co A performed causes a glitch in Co B's systems -- and the individual is not logged in on a timely basis, and thus not able to execute the sale of their rapidly dropping stock. Who's at fault? Where are the lines of liability drawn? [Attribution:* http://discuss.andredurand.com/newsItems*]*

Whether liability disclaimers would apply solely to EAP as a legal entity, or would extend to structure liability allocation between parties, such as a CSP and Relying Party, is a key scoping issue.]

5.1. Liability Disclaimers

Types of damages to address (either by disclaiming them, allocating the risk, or shifting the risk to other parties through insurance, bonding, contracts or otherwise) include: direct, indirect, incidental, special, consequential, punitive or exemplary damages, including damages fro loss of profits, revenue, good will, data, electronic orders or other economic advantage. Theories of liability to be disclaimed or otherwise addressed include contract breach, tort (including privacy breaches, trespass to chattels and negligence), and intellectual property infringement.

5.2 Liability for Inadequate Backup or Equipment

Liability for inadequate backup of data or sub-standard equipment or maintenance of equipment (including installing updates, patches or other upgrades) can be addressed separately.

5.3 Hold Harmless and Indemnity

Agreement to hold harmless, not to sue an EAP party, or the requirement to indemnify an EAP party may be addressed as part of liability. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so any such limitations would need to be tailored accordingly.

6. Authorized Use of Services

This section may set boundary condition around use of services of a CSP, Relying Party, EAP or other party to these Rules. For example, is a given CSP did not wish a direct competitor to share its customers, such a restriction could be noted here. Similarly, if it were necessary to receive a quote from a CSP defining price, quality and/or timeliness of service, such requirement and process may be noted here. A clause of this nature could be generic, applying to any EAP party, or could be partially or totally modular, allowing parties to select from among standard approved clauses reflecting how they already do business. This last approach mirrors the alternatives presented in 2.C and 3.C of the May 11, 2004 document " Business and Legal Rules in Terms Sheet: Some Alternatives for BRP Work Group".

7. Intellectual Property and Branding

Mandatory, permitted and prohibited use of the EAP or other relevant branding would be dealt with here. Licensing of the EAP marks or logos, as well as copyrights, business process patents or other trademark use would be detailed in this section. If these rules extend to underlying business factors, IP between EAP parties may also be addressed here. EXAMPLE: If a bank were to originate an authenticated user session between the bank's customer and a federal agency application from the bank's web site, then the details of framing and any bank branding affecting the federal agency web site may be dealt with here.

8. Amendments to the Terms

How these Rules are amended, by whom, with what notice and other relevant factors related to changing the terms would be addressed here.