PLASMA
Straw Man Proposals

Jim Schaad
Soaring Hawk Consulting
Requirements

• Minimize the data stored on the server
• Validate server before talking to it
• Maximize backwards interoperability
• Place all policy enforcement on servers rather than on the client
• Set of recipients can be changed post message send
• Allow multiple types of authentication
<table>
<thead>
<tr>
<th>S/MIME Recipient Info</th>
<th>KEK Recipient Info</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>New Custom Recipient</strong></td>
<td></td>
</tr>
<tr>
<td>• Allows greatest flexibility</td>
<td></td>
</tr>
<tr>
<td>• Backwards capability issue with</td>
<td></td>
</tr>
<tr>
<td>• Microsoft</td>
<td></td>
</tr>
<tr>
<td>• Thunderbird</td>
<td></td>
</tr>
<tr>
<td>• Easiest client recognition</td>
<td></td>
</tr>
<tr>
<td><strong>KEK Recipient Info</strong></td>
<td></td>
</tr>
<tr>
<td>• Overloads existing structure</td>
<td></td>
</tr>
<tr>
<td>• Backwards compatible</td>
<td></td>
</tr>
<tr>
<td>• Currently ignored recipient info</td>
<td></td>
</tr>
<tr>
<td>• Detection relatively easy</td>
<td></td>
</tr>
<tr>
<td>• Create new OtherKeyAttribute</td>
<td></td>
</tr>
</tbody>
</table>
New KEK Attribute

• SignedData
  – Encapsulated Content is EnvelopedData
    • Encapsulated Content is new content EPS-LockBox
      – Names of recipients
      – Policy to apply for recipients
      – Key Encryption Keys
  – New signed attribute – URL(s) of Policy Server
Complex Policy Structure

• Policy Identifier
  – URI or OID – to be decided
  – Need to have parameters for the policies?

• Policy Logic
  – And, or, exclude
Protocol

• Currently based on WS-Trust 1.3
  – OASIS standard
  – SOAP based
  – Requires client to manage SAML queries

• Potentially should base on ABFAB
  – Allows policy decision service to manage SAML queries
Protocol Steps Needed

Get Policies

Create KEK attribute

Policy Decision Server

Policy Enforcement Client

Decode KEK Attribute
Questions