Kerberos for the Web
Current State and Leverage Points

Executive Advisory Board Meeting
and
Financial Services Security Summit

Towards Kerberizing Web Identity and Services

1. To explain
   ▶ The identity landscape and where Kerberos might fit in.
   ▶ Our recommendations to the Kerberos Consortium.

2. To listen
   ▶ Your business cases
   ▶ Your user stories
   ▶ Your requirements
Scope

• **Towards**
  • Help MIT KC understand the web identity landscape, and Kerberos' place in it.
  • Find the right problems to solve.

• **Kerberizing**
  • Mature & highly successful intra-Enterprise technology.
  • Largely irrelevant in the Web space.

• **Web Identity**
  • Human wielding a web browser, talking to a machine.

• **Web Services**
  • Machine wielding web technologies, talking to a machine.
A Short History of Web Identity
The Primordial Identity Soup

Typically HTTP+HTML Form-based authentication
Birth of Web Single Sign-On and Identity

Typically HTTP+HTML Form-based authentication

Service provider requests IdP to perform end-user authentication
Evolution Towards Federated Identity

Typically HTTP+HTML Form-based authentication

Service provider from another domain relies on IdP to perform end-user authentication
Emergence of Web Services
Stakeholders
Stakeholders

• End Users
  • Consumers
  • Employees

• Service Providers
  • Internal-facing services consuming Employees' identities
  • External-facing services consuming Consumers’ identities

• Enterprises

• Federated Partners
# Stakeholder Requirements

<table>
<thead>
<tr>
<th>Stakeholders</th>
<th>Type</th>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>End users</td>
<td>Simplicity</td>
<td>U1</td>
<td>End users want to reduce the number of sign-on technologies and credentials that they are required to use to access web-based service providers.</td>
</tr>
<tr>
<td></td>
<td>Transparency</td>
<td>U2</td>
<td>End users want to reduce the number of authentication steps taken when using service providers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>U3</td>
<td>End users want to use mobile devices when authenticating to service providers.</td>
</tr>
<tr>
<td></td>
<td>Flexibility</td>
<td>U4</td>
<td>End users want to assert different identity information in different contexts, e.g. to be able to &quot;don&quot; different roles when interacting with either the same or different service providers (e.g. to be able to interact with a given bank in the role of either an individual consumer, or an officer of a company which is also the same bank's customer).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>U5</td>
<td>End users want to use untrusted devices (e.g. an airport Internet kiosk or a borrowed device) to access service providers without compromising their credentials.</td>
</tr>
</tbody>
</table>
## Stakeholder Requirements

<table>
<thead>
<tr>
<th>Stakeholders</th>
<th>Type</th>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Service Providers</strong></td>
<td>Simplicity</td>
<td>S1</td>
<td>Service providers that consume identities from third-party identity providers want to reduce and/or minimize the number of sign-on technologies that they are required to support. This applies to both Internet-based and enterprise-based SPs.</td>
</tr>
<tr>
<td></td>
<td>Risk management</td>
<td>S2</td>
<td>Service providers want to be able to manage and minimize the risks they assume in providing their service, particularly with respect to phishing in Financial services and similarly sensitive applications.</td>
</tr>
</tbody>
</table>
# Stakeholder Requirements

<table>
<thead>
<tr>
<th>Stakeholders</th>
<th>Type</th>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise</td>
<td>Risk management</td>
<td>E1</td>
<td>Enterprise security officers want secure authentication for SOA.</td>
</tr>
<tr>
<td></td>
<td>E2</td>
<td>E2</td>
<td>Enterprise SOA architects want flexible life-cycle management for identities used for SOA.</td>
</tr>
<tr>
<td></td>
<td>E3</td>
<td>E3</td>
<td>Enterprise administrators want to reuse existing Kerberos infrastructure when deploying web applications and web services in order to reduce the cost of security administration.</td>
</tr>
<tr>
<td></td>
<td>E4</td>
<td>E4</td>
<td>Enterprise system integrators want interoperability between web service implementations from major vendors.</td>
</tr>
<tr>
<td></td>
<td>E5</td>
<td>E5</td>
<td>Enterprise identity architects want SSO-support in popular browsers with credential delegation capabilities turned on by default.</td>
</tr>
<tr>
<td>N-Tier</td>
<td>E6</td>
<td>E6</td>
<td>Enterprise identity architects want to be able to extend existing cookie-based SSO systems with support for Kerberos backchannel authentication and credentials delegation.</td>
</tr>
</tbody>
</table>
# Stakeholder Requirements

<table>
<thead>
<tr>
<th>Stakeholders</th>
<th>Type</th>
<th>Code</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Federated Partners</td>
<td>N-tier</td>
<td>F1</td>
<td>Deployers of web-based portal services with kerberized backend-services need to be able to use federated identity with N-tier authentication.</td>
</tr>
<tr>
<td></td>
<td>Level of Authentication</td>
<td>F2</td>
<td>Grid services (in environments where PK-INIT is used) in the US Federal sector need to fulfill policy requirements that authentication be done using smartcards.</td>
</tr>
<tr>
<td></td>
<td>Identity Provider Discovery</td>
<td>F3</td>
<td>Service providers with a large number of affiliated Identity Providers requires a way to determine which Identity Provider a user is affiliated with, so that it knows where to request assertions for the user'.</td>
</tr>
<tr>
<td></td>
<td>Technical trust establishment</td>
<td>F4</td>
<td>Federated partners want to reduce the complexity and effort incurred in establishing technical trust between their systems.</td>
</tr>
<tr>
<td></td>
<td>Governance</td>
<td>F5</td>
<td>The IT management at two or more federated partners need to define conventions, or an agreement, governing the use of a federated business process that is secured using Kerberos.</td>
</tr>
</tbody>
</table>
Use cases
Back channel

Web service client

Web service

Shared secrets often stored insecurely and poorly managed

Enterprise infrastructure (KDC, etc)

Web services not integrated into Enterprise infrastructure
Front channel

Increasing demand for mobile or untrusted devices

Secure and single sign on, but selective.

Discovery of identity provider in multi-party federations

Ability to converse with a diverse range of identity providers
Technology
Aspects & Technology

• Front-channel Authentication
• Message Authentication/Message Security
• Credentials Delegation
• Level-of-Assurance Transport
• Identity Federations
Aspects & Technology

- **Front-channel Authentication**
  - Negotiate
  - Information Card
- **Message Authentication/Message Security**
- **Credentials Delegation**
- **Level-of-Assurance Transport**
- **Identity Federations**
Aspects & Technology

- Front-channel Authentication
- **Message Authentication/Message Security**
  - WS-Security Kerberos Token Profile
- Credentials Delegation
- Level-of-Assurance Transport
- Identity Federations
Aspects & Technology

- Front-channel Authentication
- Message Authentication/Message Security
- **Credentials Delegation**
  - Kerberos and the Enterprise Web SSO
  - Constrained Delegation (s4u2self)
- Level-of-Assurance Transport
- Identity Federations
Aspects & Technology

- Front-channel Authentication
- Message Authentication/Message Security
- Credentials Delegation
- Level-of-Assurance Transport
  - SAML Authentication Context
- Identity Federations
Aspects & Technology

• Front-channel Authentication
• Message Authentication/Message Security
• Credentials Delegation
• Level-of-Assurance Transport
• Federated Identity
  • SAML
  • OAuth
  • OpenID
Opportunities
Opportunities

Front channel

End-user

Authentication using TLS+KRB (O1); Negotiate (O2); Kerberos-augmented Information Card (O3+O5) or OpenID (O8); also document and promote (O12).

Trust established using OpenID +KRB bootstrap (O9); SAML metadata (O11).

Delegation using OAuth augmented with SAML or Kerberos (O6).

Authentication using Negotiate (O2); Kerberos Token Profile (O10); SAML-in-KRB (O14) or KRB-in-SAML (O13) or SAML-in-GSSAPI (O16).

Trust established using OAuth+KRB bootstrap (O7); SAML metadata (O11).

Another service

End-user Identity Provider and/or KDC

Service provider

Authentication using TLS+KRB (O1), Negotiate (O2), Kerberos-augmented InfoCard (O4+O5) or OpenID (O8) or SAML; SAML-in-KRB (O14) or KRB-in-SAML (O13) or SAML-in-GSSAPI (O16).

Discovery using asserted realm (O15)

© 2007 The MIT Kerberos Consortium. All Rights Reserved.

3-4 November 2008
Analysis and Recommendations
Back channel use cases

• SOAP
  – Update WS-Security Kerberos Token Profile

• REST & Plain XML
  – SAML-in-Kerberos (over Negotiate or TLS handshake).

• Federated use-cases require improved cross-realm operation.
Front channel use cases

• “Complementary Kerberos” or “King Kerberos”...

• Both directions require improved cross-realm operation and improved client support for multiple concurrent identities.
“Complementary Kerberos”

• Primary features
  – Strong authentication using Kerberos to a identity provider.
  – Supplements a SAML assertion’s semantics by providing Kerberos-based attestation for a user’s identity.

• A Web SSO profile (SAML, InfoCard, OpenID, etc) encapsulates and transports the attestation.
“King Kerberos”

• Primary features
  – Kerberos is used directly between the client and the service provider.
  – SAML assertion is used to decorate a Kerberos ticket, or otherwise supplement it.
  – Scope for use outside of the Web context (e.g. federated NFSv4).

• Similar to how Kerberos is used conventionally.

• Requires significant client updates
  – anonymous tickets; possibly changes to TLS / GSS providers.
Analysis

• Back channel use cases are more soluble and more likely to yield results sooner than the Front channel use cases.

• Therefore, focus on common dependencies with initial emphasis on Back channel use cases.

• Front channel strategy requires a decision between "King Kerberos" or "Complementary Kerberos".

• Our analysis suggests that overall risk and effort is similar for both approaches, but "Complementary Kerberos" is likely to yield results sooner.
Recommendations

- Recommendation 1
  “Determine the overall strategic approach in consultation with relevant stakeholders”

- Recommendation 2
  “Initiate activities to address those opportunities whose applicability is independent of strategic direction”

- Recommendation 3
  “Plan and prioritize the most critical subsequent activities”

- Recommendation 4
  “Develop an overall architecture”
Conclusions

Thank you for your attention.

Possible discussion points

Have we covered the relevant technologies?
Did we capture the requirements and use-cases?
What are the business cases?