Kerberos for the Web

Current State and Leverage Points

Executive Advisory Board Meeting

and

Financial Services Security Summit

New York, 3-4 November 2008.

Kerberos consortium
www.kerberos.org

“Towards Kerberizing Web Identity and Services”

Kerberos consortium

Towards Kerberizing Web Identity and Services

Abstract

Draft of 29-Oct-2008

Today authentication and authorization are addressed in an incoherent, and often site-specific, fashion on the Internet and the Web specifically. This situation stems from many factors including the evolution, design, implementation, and deployment history of HTTP and HTTP-based systems in particular, and Internet protocols in general.

Kerberos is a widely-implemented and widely-deployed authentication substrate with a long history in various communities and vendor products. Organizations that currently use Kerberosas a key element of their infrastructure wish to take advantage of its unique benefits while moving to Web-based systems, but have had limited success in doing so.

In this document we outline the evolution of Web Identity and Services and describe the issues surrounding this complex landscape. These issues are captured within a set of more specific requirements that are deemed necessary to satisfy the relevant stakeholders; these requirements arethen framed within the context of some general use cases. We then propose and describe a number of activities that leverage Kerberos to realize these improvements, and present an overall strategy and architectural model for working towards a more cohesive and widely deployed Kerberos-based Web authentication infrastructure.

Authors (alphabetical):

Jeff Hodges
Josh Howlett, JANET
Leif Johansson
RL "Bob" Morgan, Internet2

Introduction

In this paper we attempt to provide a high level overview of how authentication, and to a lesser extent authorization, fits into today's Web landscape and explain Kerberos' place in that landscape. We follow with a brief presentation of "user stories" -- simple statements of what end users, service providers and enterprises desire in terms of their security related experienceswhen using the Web. Next, we describe a number of use cases that are intended to place these requirements within the context of typical scenarios. A number of specific

[DRAFT] Page 1 of 34

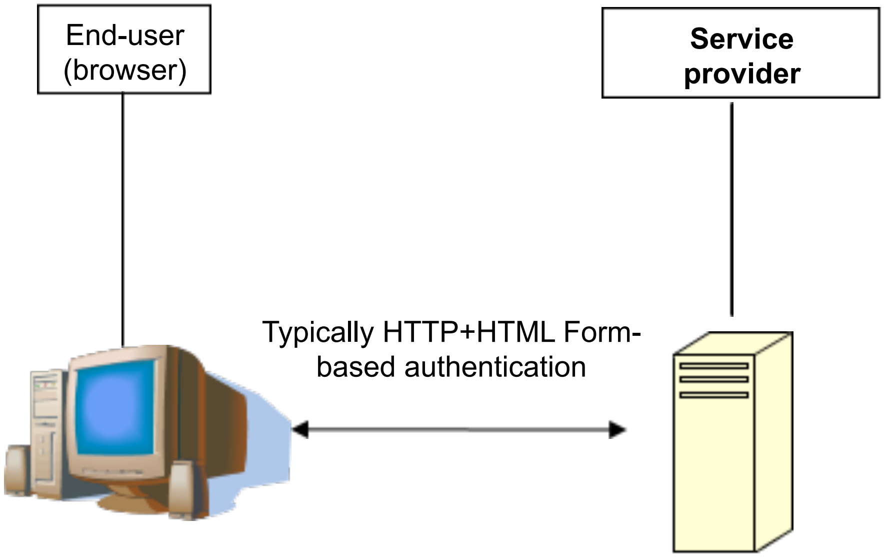
1. To **explain**
   - The identity landscape and where Kerberos might fit in.
   - Our recommendations to the Kerberos Consortium.
2. To **listen**
   - Your business cases
   - Your user stories
   - Your requirements

Scope

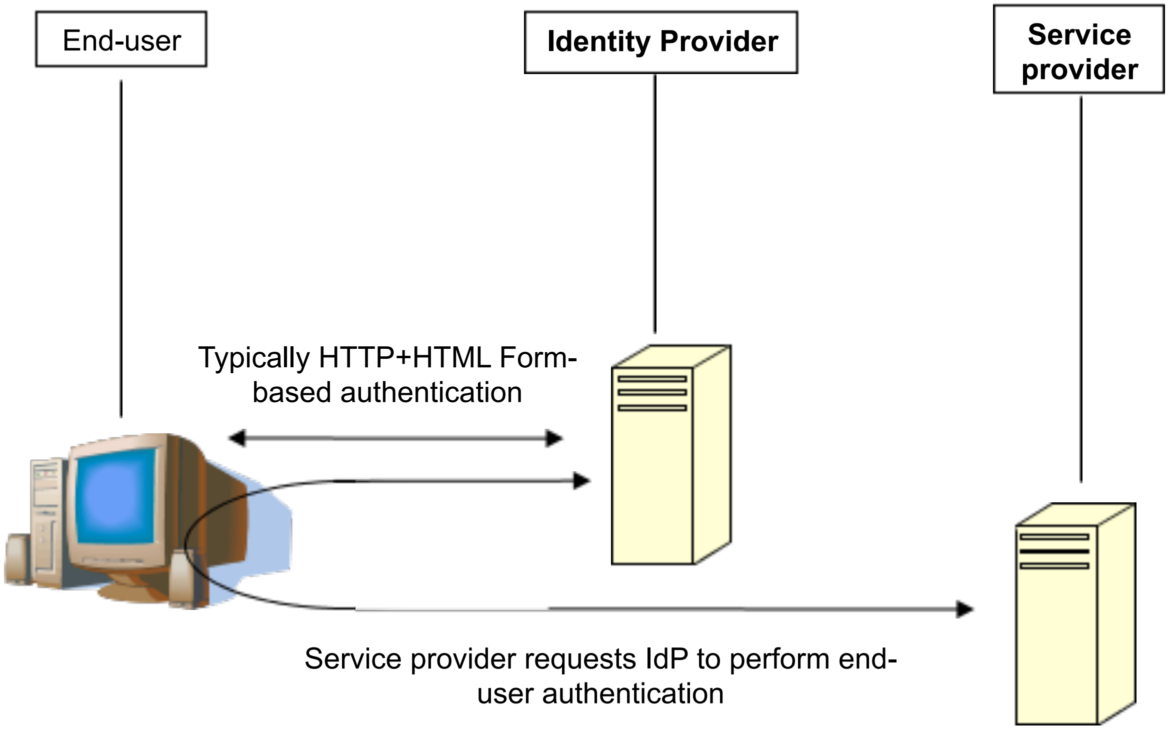
- *Towards*
  - Help MIT KC understand the web identity landscape, and Kerberos' place in it.
  - Find the right problems to solve.
- *Kerberizing*
  - Mature & highly successful intra-Enterprise technology.
  - Largely irrelevant in the Web space.
- *Web Identity*
  - Human wielding a web browser, talking to a machine.
- *Web Services*
  - Machine wielding web technologies, talking to a machine.

A Short History of Web Identity

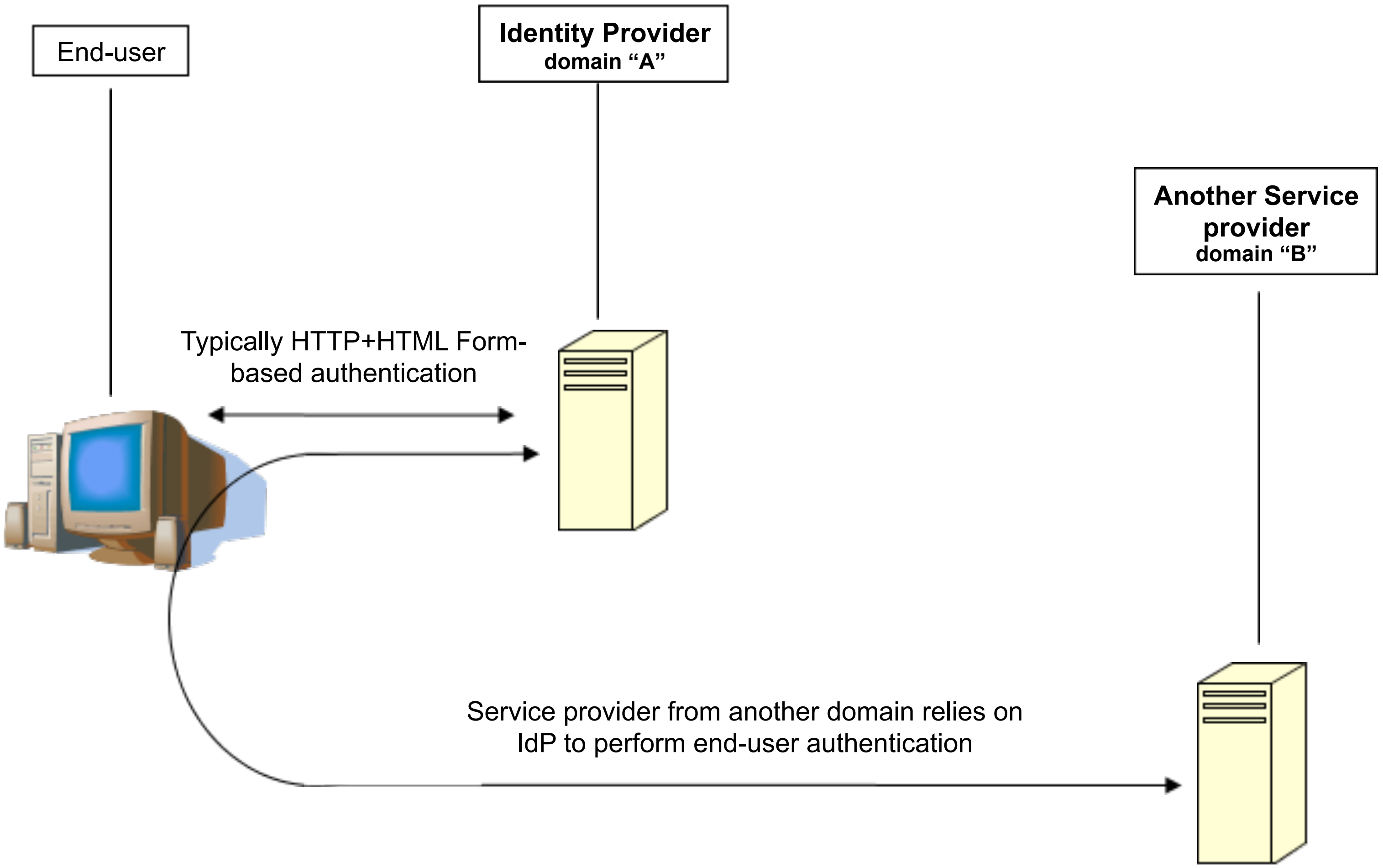
The Primordial Identity Soup



Birth of Web Single Sign-On and Identity


End-user
Identity Provider
Service provider
Typically HTTP+HTML Form-based authentication
Service provider requests IdP to perform end-user authentication

Evolution Towards Federated Identity



End-user

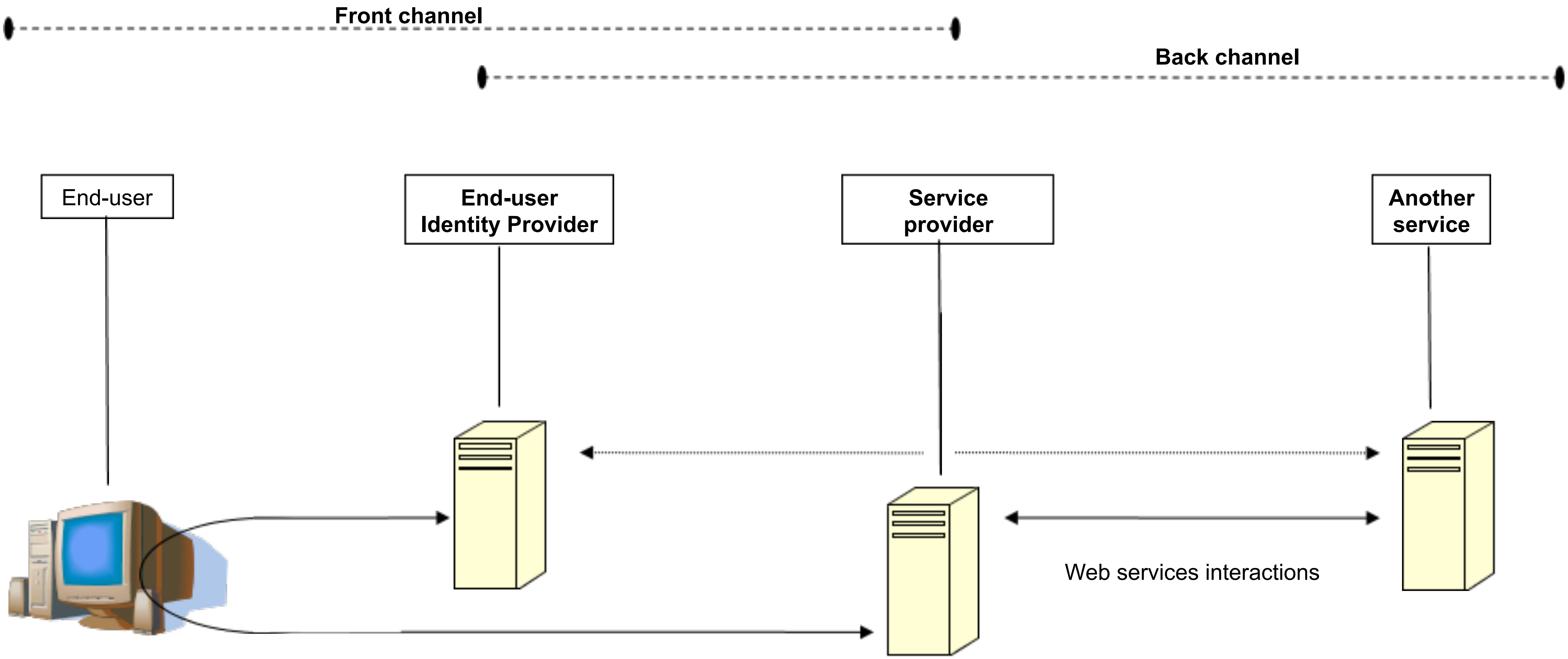
Identity Provider
domain "A"

Another Service provider
domain "B"

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

Stakeholders	Type	Code	Description
End users	Simplicity	U1	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.
	Transparency	U2	End users want to reduce the number of authentication steps taken when using service providers.
		U3	End users want to use mobile devices when authenticating to service providers.
	Flexibility	U4	End users want to assert different identity information in different contexts, e.g. to be able to "don" 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).
		U5	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.

Stakeholder Requirements

Stakeholders	Type	Code	Description
Service Providers	Simplicity	S1	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.
	Risk management	S2	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.

Stakeholder Requirements

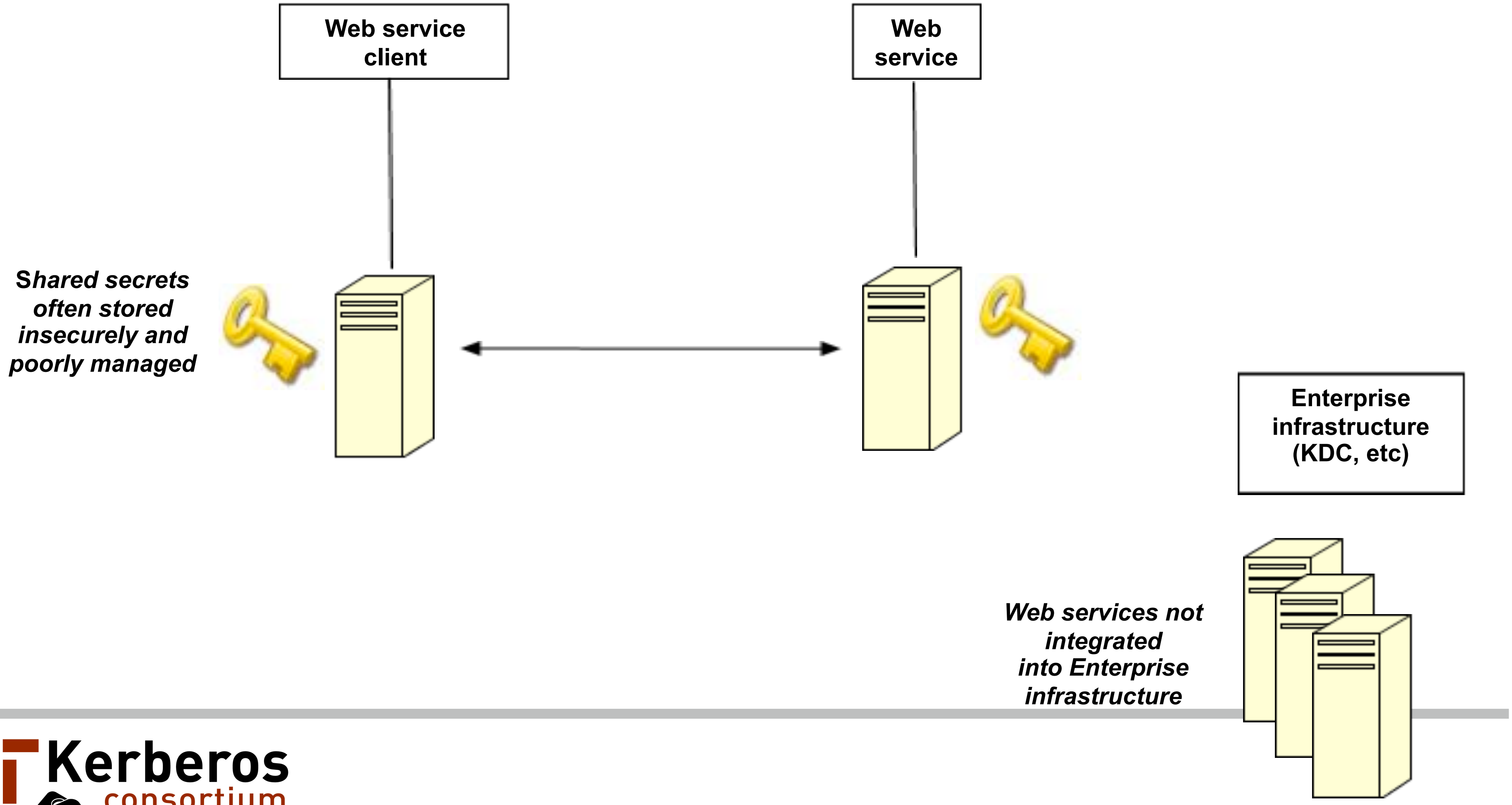
Stakeholders	Type	Code	Description
Enterprise	Risk management	E1	Enterprise security officers want secure authentication for SOA.
	Simplicity	E2	Enterprise SOA architects want flexible life-cycle management for identities used for SOA.
		E3	Enterprise administrators want to reuse existing Kerberos infrastructure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

Stakeholder Requirements

Stakeholders	Type	Code	Description
Federated Partners	N-tier	F1	Deployers of web-based portal services with kerberized backend-services need to be able to use federated identity with N-tier authentication.
	Level of Authentication	F2	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.
	Identity Provider Discovery	F3	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'.
	Technical trust establishment	F4	Federated partners want to reduce the complexity and effort incurred in establishing technical trust between their systems.
	Governance	F5	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.

Use cases

Back channel



Web service client

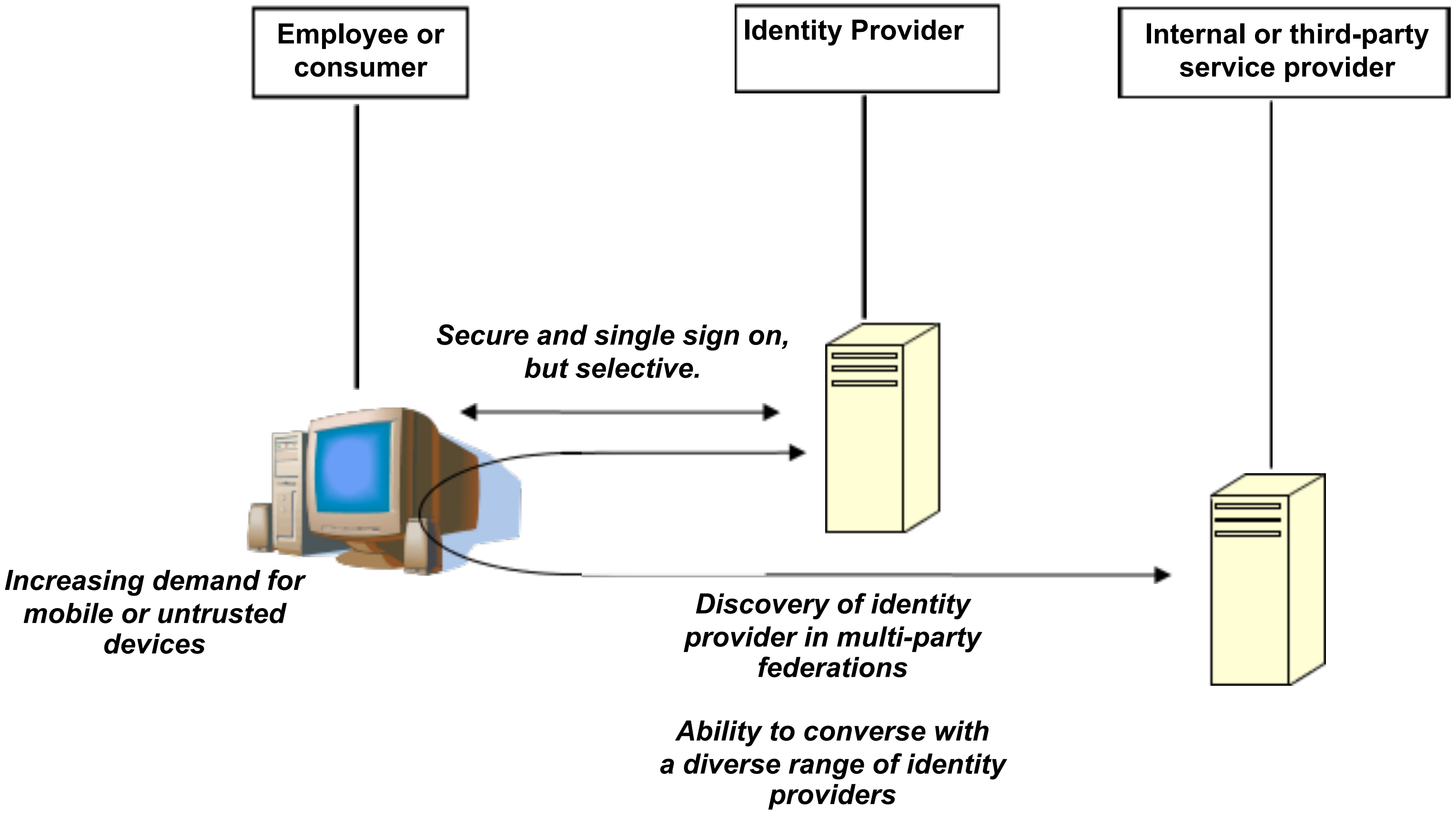
Web service

Shared secrets often stored insecurely and poorly managed

Enterprise infrastructure (KDC, etc)

Web services not integrated into Enterprise infrastructure

Front channel



Employee or consumer

Identity Provider

Internal or third-party service provider

Secure and single sign on, but selective.

Increasing demand for mobile or untrusted devices

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

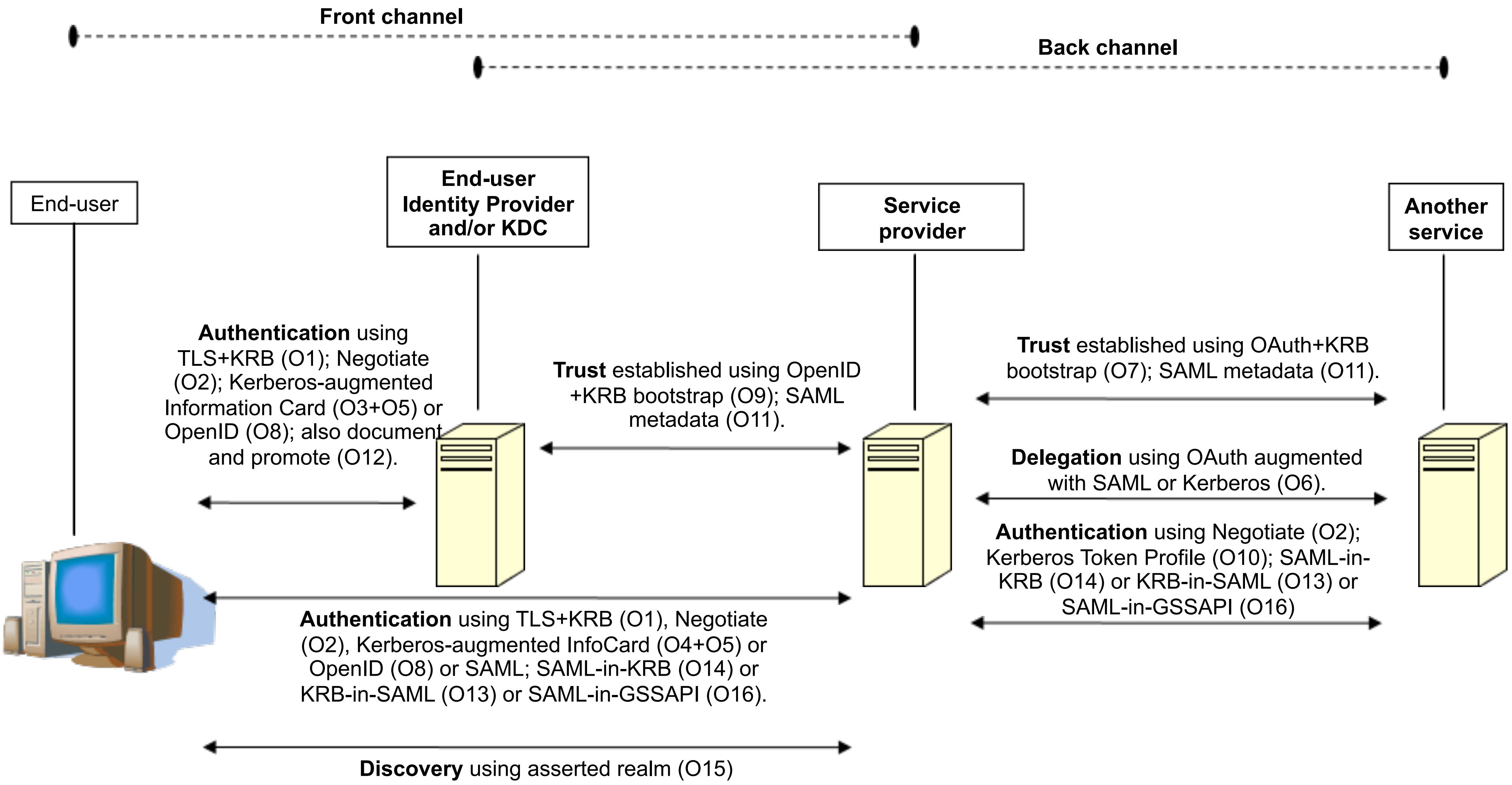
- Front-channel Authentication
- Message Authentication/Message Security
- Credentials Delegation
- **Level-of-Assurance Transport**
    - SAML Authentication Context
- Identity Federations

Aspects & Technology

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

Opportunities

Opportunities



Front channel

Back channel

End-user

End-user Identity Provider and/or KDC

Service provider

Another service

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).

Trust established using OAuth+KRB bootstrap (O7); 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)

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)

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?