enspier
TECHNOLOGIES

Using Digital Certificates to Establish Federated Trust

chris.brown@enspier.com

**U.S. E-Authentication Interoperability
Lab Engineer**

Agenda

- U.S. Federal E-Authentication Background
- Current State of PKI in E-Authentication
- Future of PKI in E-Authentication
- Conclusion

enspier TECHNOLOGIES

E-Authentication Background

- What is E-Authentication?
- Federal documents that support E-Authentication
- Protocol Background
- E-Authentication Interoperability Lab

What is E-Authentication?

- Trusted and secure standards-based authentication architecture
- Focuses on meeting the authentication business needs of the U.S. E-Government initiatives
- Based on U.S. Government documents M-04-04 and SP800-63

M-04-04

- Defines four assurance levels:
  - 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
  - Level 4: Very high confidence in the asserted identity’s validity

enspier TECHNOLOGIES

M-04-04

- Risk Assessment
  - Risk based on impact categories

enspier TECHNOLOGIES

Special Publication 800-63

- Provides technical guidance to U.S. agencies.
- Defines what authentication mechanisms can be used for each assurance level.

Special Publication 800-63

- Level one and two assurance levels:
  - Generally password/pin based
  - Level one requires protection of the of the credential, but does not require identity proofing
- Level three and four assurance levels:
  - Typically cryptographic based authentication (X.509 certificates)
  - Level four assurance level must be a hard token (e.g. smartcard)

enspier TECHNOLOGIES

E-Authentication Background

- 31 operational applications.
- Trust is the key:
  - Applications must trust Identity Providers
  - Identity Providers must trust applications
- Privacy must be maintained

enspier TECHNOLOGIES

Protocol Background

- Adopted the Browser Artifact Profile of the SAML 1.0 protocol
- E-Authentication has it’s own nomenclature:
    - Relying Party = Service Provider
    - Credential Service = Identity Provider

Protocol Background

- Mutually authenticated TLS chosen to secure communications between the service provider and identity provider
- Service providers can not interoperate with an identity provider of a lower assurance level
- Three separate certificate authorities were established by the U.S. Government

E-Authentication Interoperability Lab

- Experts in the federated identity technology
- The lab works with COTS Identity and Access Management software products that are used to perform identity federation
- Consult with Federal agencies who are implementing identity federation with E-Authentication.
- The E-Authentication interoperability laboratory is the only known facility in the world that provides these services.

enspier
TECHNOLOGIES

Agenda

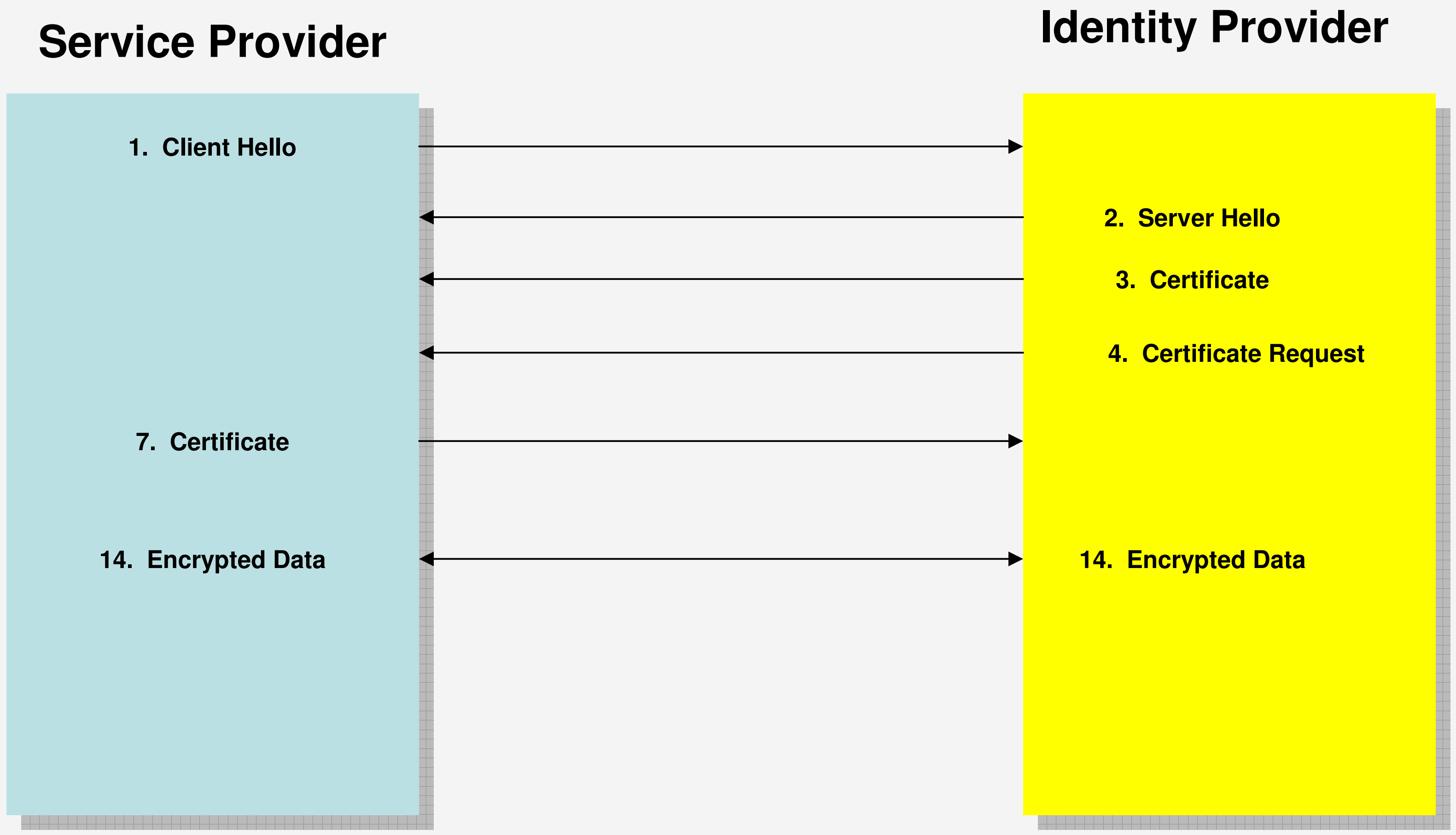
- U.S. Federal E-Authentication Background
- **Current State of PKI in E-Authentication**
- Future of PKI in E-Authentication
- Conclusion

enspier
TECHNOLOGIES

Current State of PKI in E-Authentication

- PKI Credentials are used for authentication between service providers and identity providers
  - Mutual TLS presents hurdles
  - Path validation engines are not robust
- PKI Credentials are used as the basis of certificate based authentication of end users at E-Authentication level 3 and 4.

Mutual TLS Overview



Service Provider

Identity Provider

1. Client Hello

2. Server Hello

3. Certificate

4. Certificate Request

7. Certificate

14. Encrypted Data

14. Encrypted Data

PKI Issues

- PKI is not a well known subject among engineers
  - Asymmetric/Symmetric cryptography
  - ‘Private’ Keys
  - Passwords

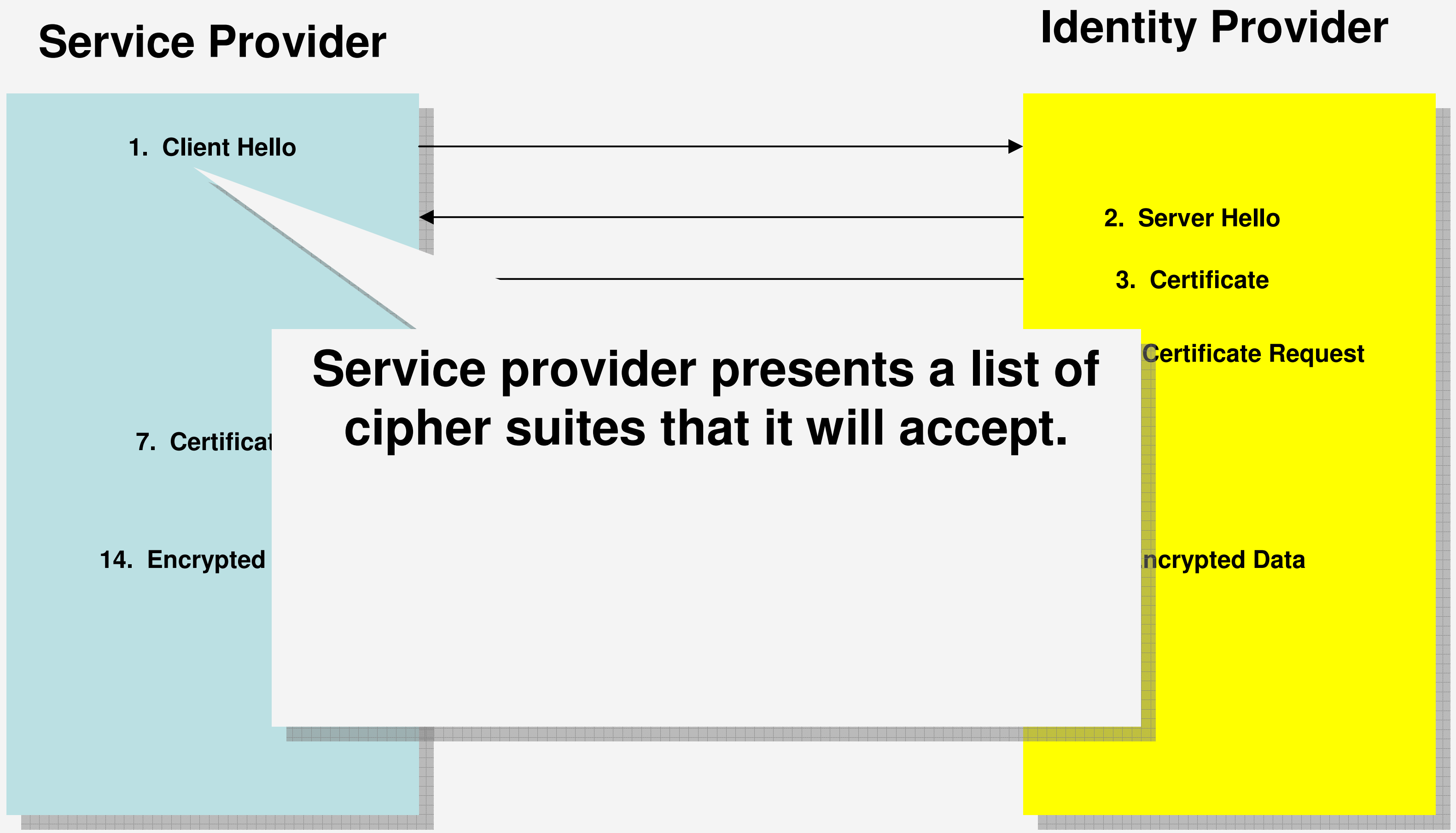
PKI Issues

- Web servers have differences in implementation of TLS
  - Configuration not intuitive
  - Implementations are ‘buggy’
  - Troubleshooting is hard

TLS Anecdote #1 – Certificate Formatting

- As an IdP, one product would deny all client (service provider) certificates.
- “not signing certificate” written to IdP log file
- Lab determined that all certificates with the “id-kp-clientAuth” (client authentication) bit set in the extended key usage extension were rejected by the IdP.
- Extension bit is allowed by TLS and the EGCA profile
- Trouble ticket opened/patch issued

TLS Anecdote #2 – Cipher Suites



Service Provider

Identity Provider

1. Client Hello

2. Server Hello

3. Certificate

Certificate Request

7. Certificat

14. Encrypted

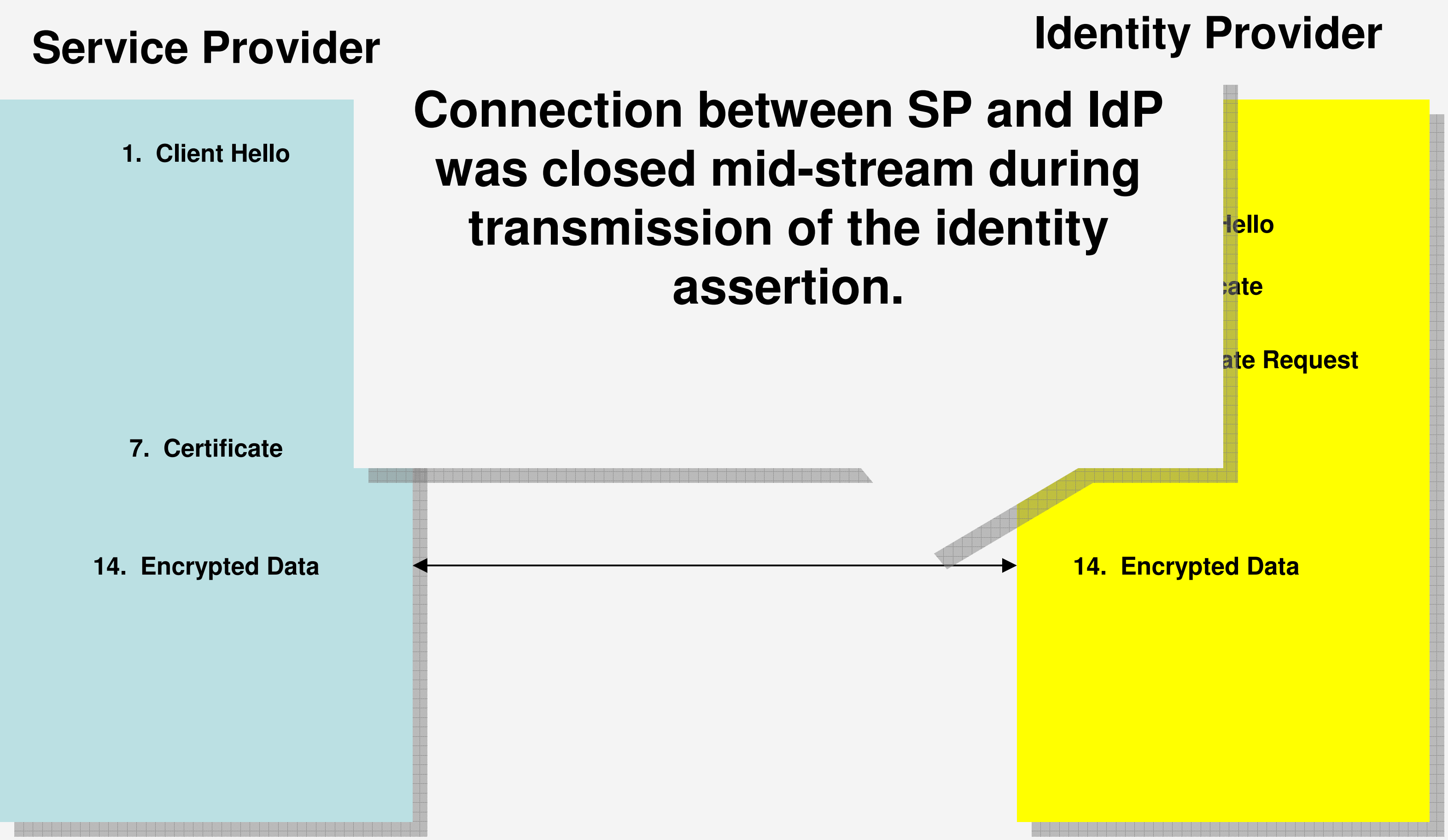
ncrypted Data

Service provider presents a list of cipher suites that it will accept.

TLS Anecdote #2 – Cipher Suites

- ‘Weak’ cipher suites are sent from the SP to the IdP (MD5withRC4)
- IdP web servers often pick the ‘weak’ cipher
- Only FIPS-approved algorithms should be used in E-Authentication transactions
- No SP products can be configured to send approved cipher suites
- IdP web servers should be configured to accept only FIPS approved algorithms or end the negotiation

TLS Anecdote #3 – Algorithm Mismatch



Service Provider

Identity Provider

1. Client Hello

7. Certificate

14. Encrypted Data

ello

ate

ate Request

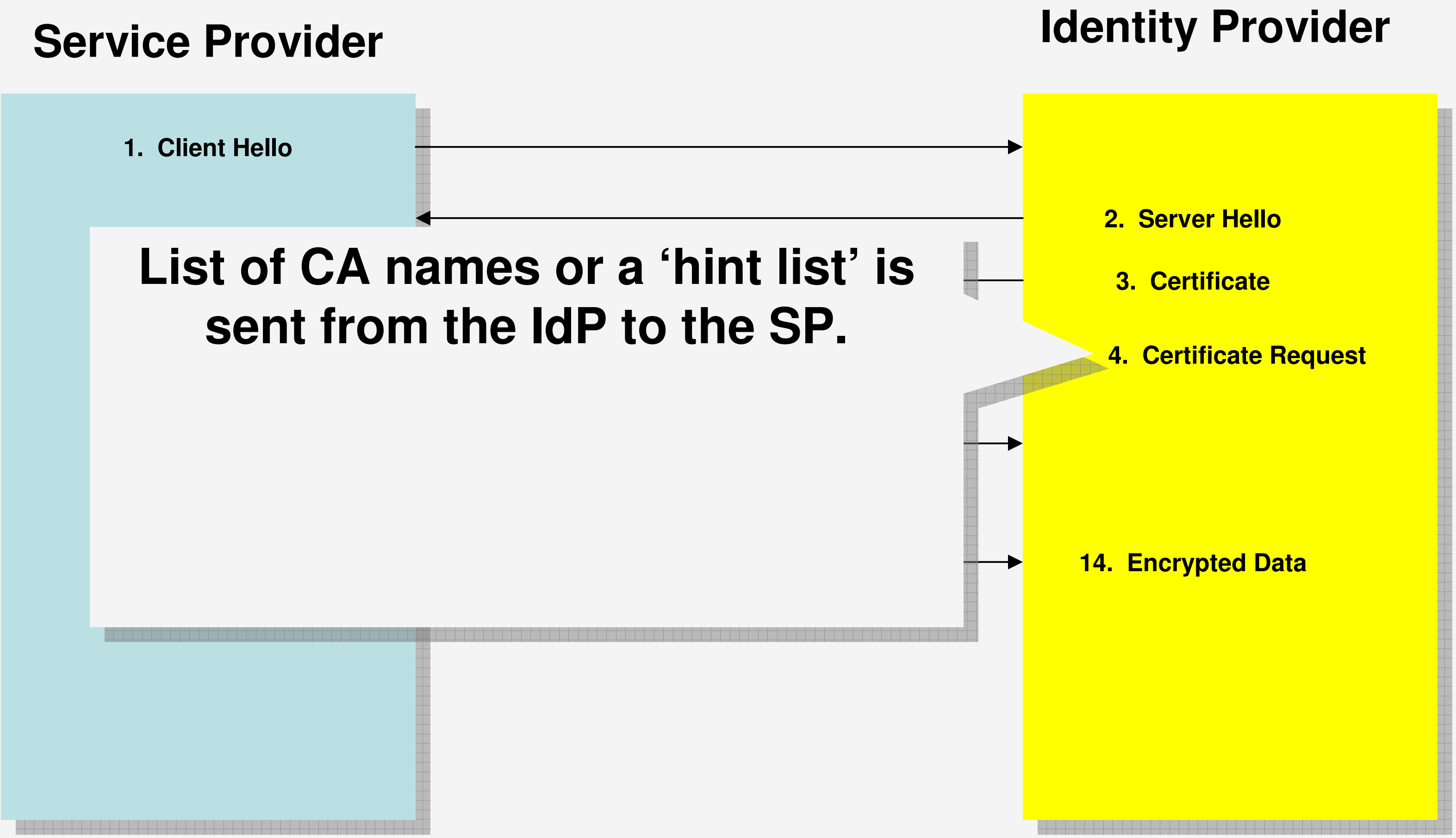
14. Encrypted Data

Connection between SP and IdP was closed mid-stream during transmission of the identity assertion.

TLS Anecdote #3 – Algorithm Mismatch

- During testing, an E-Authentication IdP used a toolkit that was not tested by the Interoperability Lab.
- Lab used an open source tool that decrypted TLS traffic to debug.
- SP presented Cipher Block Chaining based cipher suites that had vulnerabilities.
- SP software was not updated to address vulnerabilities

TLS Hint List



Service Provider

Identity Provider

1. Client Hello

2. Server Hello

3. Certificate

4. Certificate Request

14. Encrypted Data

List of CA names or a ‘hint list’ is sent from the IdP to the SP.

TLS Hint List

- Requires the IdP to import the correct CA certificate into their trust store.
- Often, the wrong certificate is imported.

Mutually Authenticated TLS – Conclusion

- Mutually authenticated interoperability problems are not uncommon and not straightforward to troubleshoot
- Patches from vendors require ‘recertification’.
- Time and money consuming issue for all members of the E-Authentication

Certificate Revocation

- Certificate revocation list checking feature is lacking in many SAML 1.0 aware products
- SPs should check CRLs in case IdP keys become compromised
- SP/IdP connections are managed in a manual way

Certificate Revocation

- U.S. agencies with strict security requirements have written their own CRL checking software
- Two approaches to CRL checking:
  - LDAP directory
  - AIA extension
- Products are now tested for CRL checking functionality

enspier TECHNOLOGIES

FIPS Requirement

- U.S. Government agencies are restricted by Federal Information Processing Standards publication 140-2 (***Security Requirements for Cryptographic Modules)***. Generated keys must be FIPS 140-2 compliant.
- FIPS approved modules are often expensive for a federal agency. Open source toolkits exist (OpenSSL, NSS, Crypto++) but require programming.

E-Authentication PKI Testing Approach

- SAML products and assertion based identity providers and service providers are tested to determine if they implement the proper mechanisms to assure privacy and trust.
- Service Providers are tested against three different types of SAML assertion responders.
  - ‘Friendly’ error must be captured
- Identity Providers are tested against three different types of Service Provider client certificates.
  - Requirements are easier to meet.
  - CRL checking is configurable by the web/application server

enspier
TECHNOLOGIES

E-Authentication PKI Testing Approach

- Level two service providers are tested that they don’t accept assertions from level one identity providers.
- All identity providers are tested that they do not issue assertions over a non mutual TLS channel.

Agenda

- U.S. Federal E-Authentication Background
- Current State of PKI in E-Authentication
- **Future of PKI in E-Authentication**
- Conclusion

PKI Enhancements to the E-Authentication Adopted Scheme

- SAML 2.0 requests will be signed. SAML 2.0 responses will be signed and encrypted.
  - Application layer security preferred
  - Removes reliance on web server cryptographic configuration

enspier
TECHNOLOGIES

PKI Enhancements to the E-Authentication Adopted Scheme

- Mutually authenticated TLS only provides endpoint to endpoint security
  - assertions in plain text in log
- Web services forward messages to other services
- IdP could request attribute at SP1 on behalf of SP2.
  - User’s nameIdentifier at SP2 is unknown by SP1 because it is encrypted by the IdP.

PKI Enhancements to the E-Authentication Adopted Scheme

- SAML Vendor Wish list
  - ‘Pluggable’ path validation and discovery engine
    - Engines are capable of discovering paths through complex bridge environments.
  - CRL checking
  - Certificate policy processing
    - Eliminates the need for separate IdP certificate authorities.

PKI Enhancements to the E-Authentication Adopted Scheme

- ‘web-of-trust’ is another proposed solution to trust between members of E-Authentication
  - No extensive path processing necessary
  - CRL problem must be solved

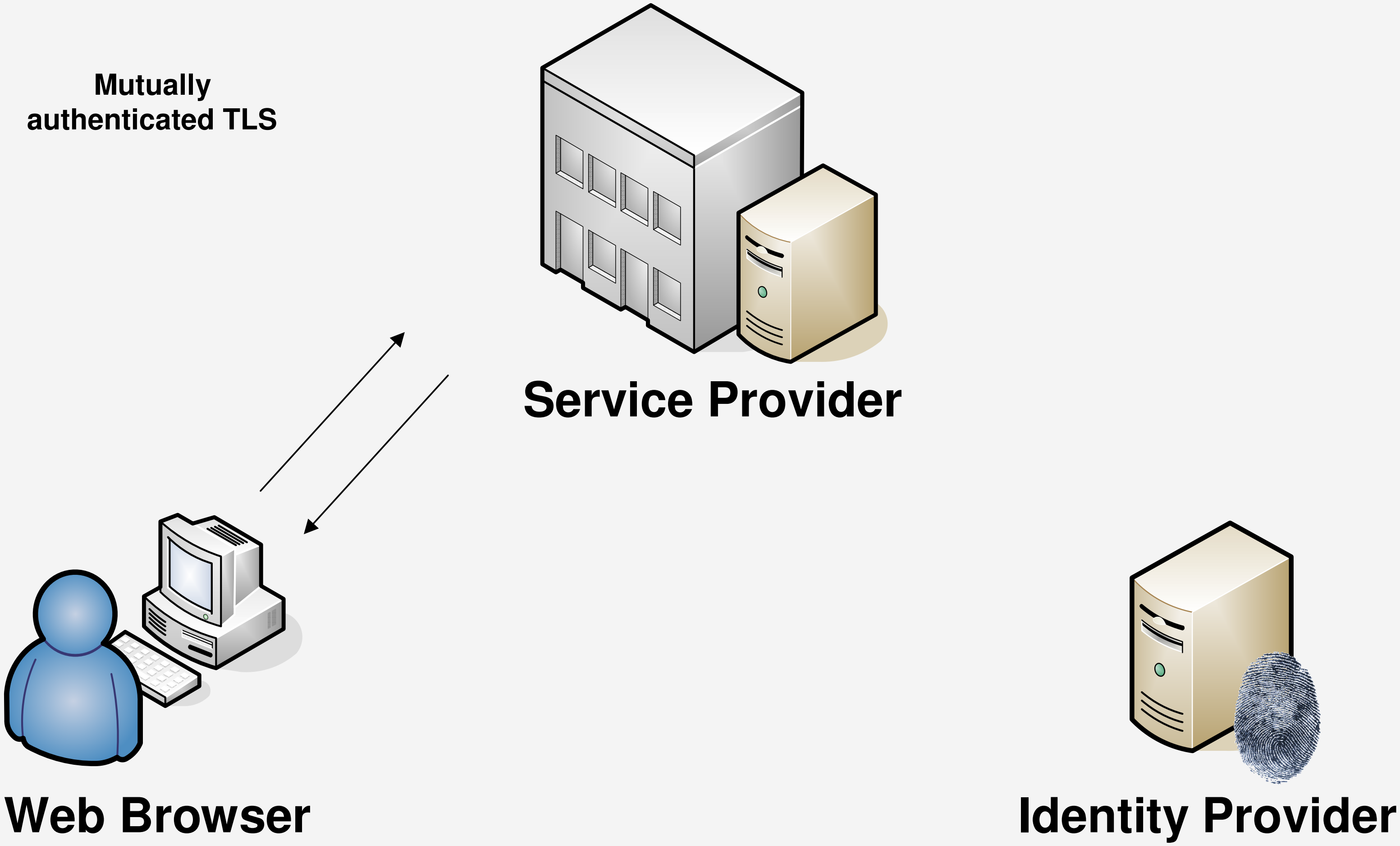
X.509 Based Authentication and User Attributes

- Service Providers need more user information
  - access control
  - activation
- PKI credential accepting service providers must take advantage of the already existing SAML infrastructure in the E-Auth federation.

SAML Attribute Authority Private Extension

- Extension contains a URL pointing the service provider to the IdP metadata.

SAML Attribute Authority Private Extension



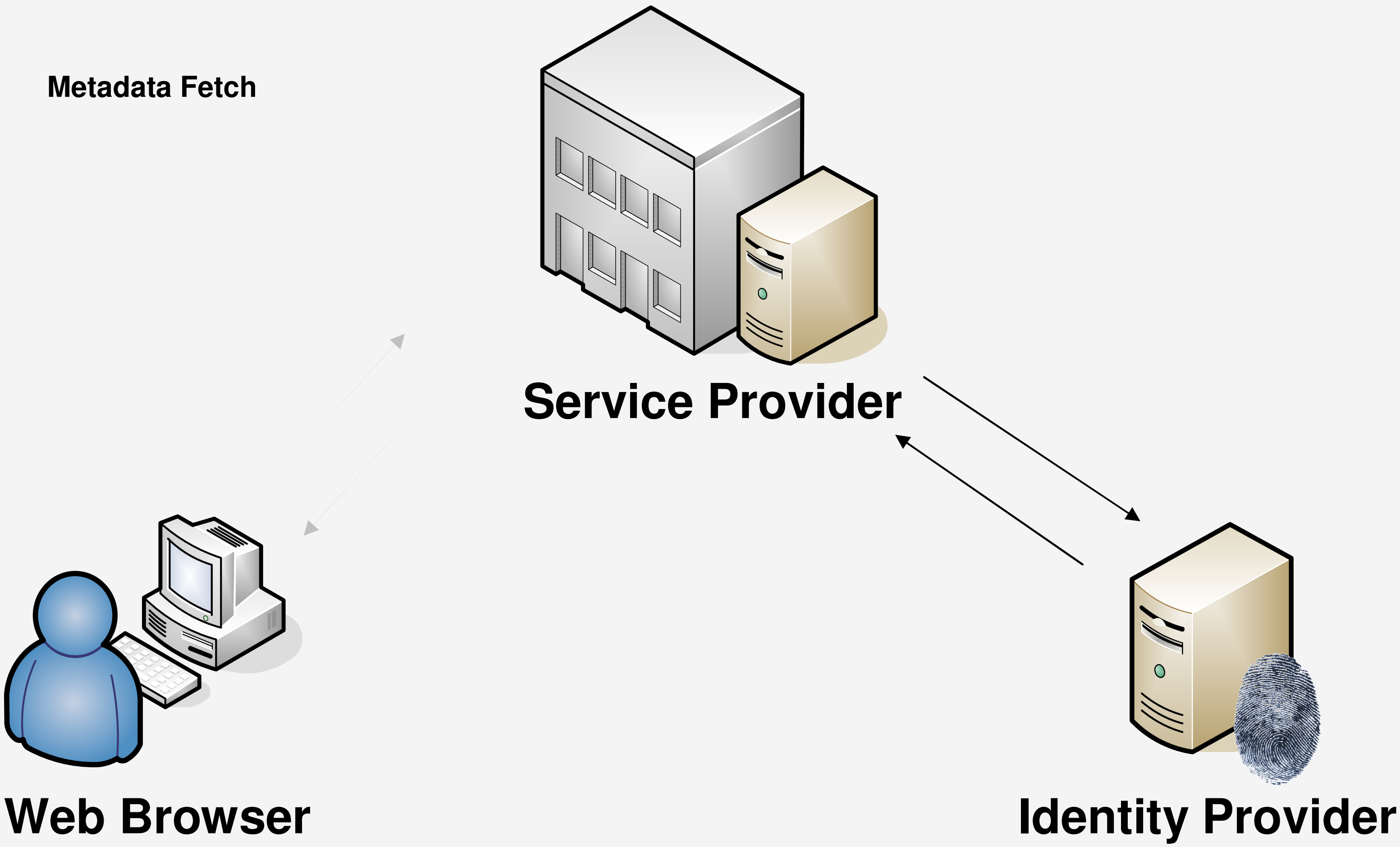
Mutually authenticated TLS

Service Provider

Web Browser

Identity Provider

SAML Attribute Authority Private Extension



Metadata Fetch

Service Provider

Web Browser

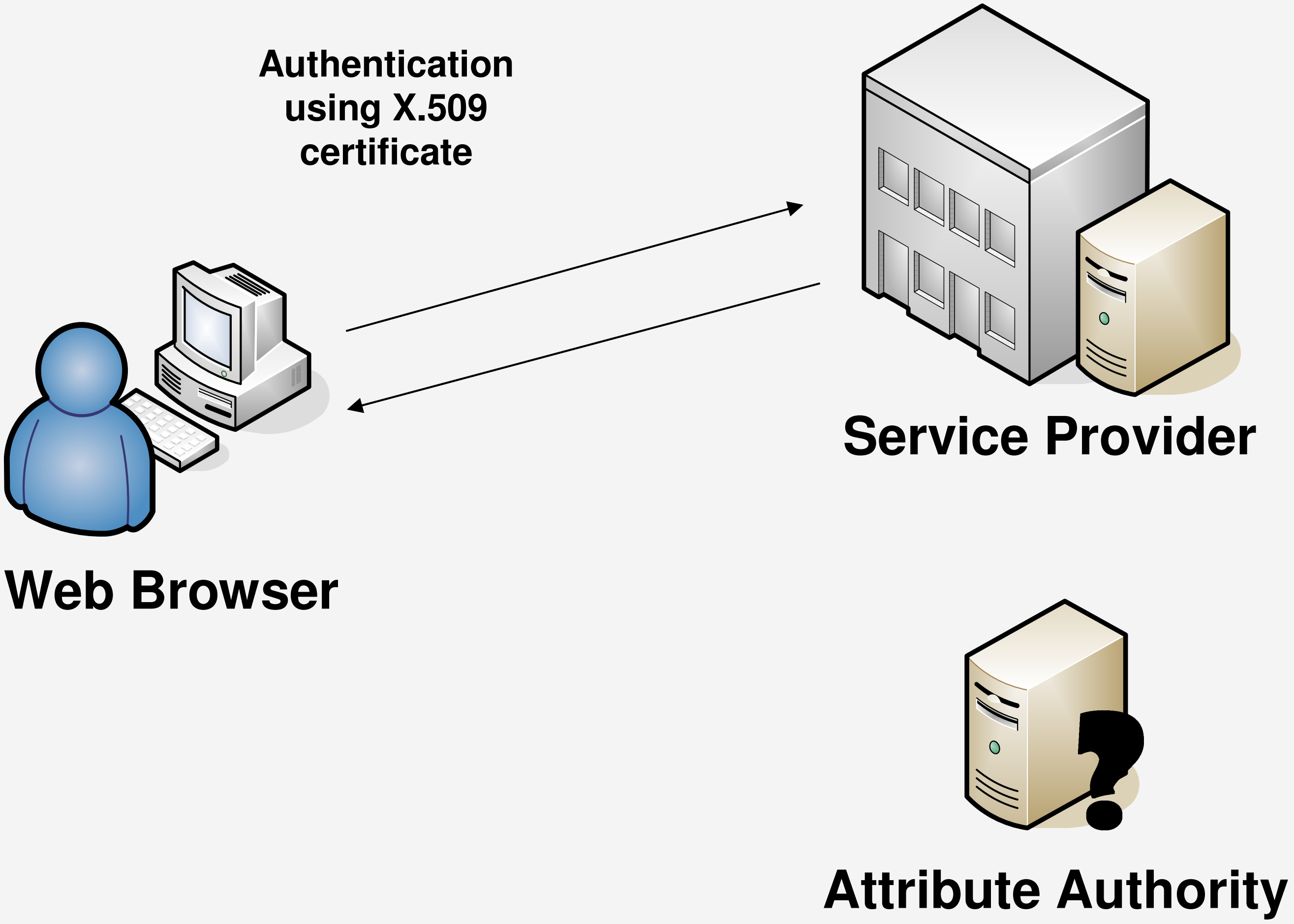
Identity Provider

SAML Attribute Authority Private Extension

- <AttributeAuthorityDescriptor> is located within the metadata
- User can sign the <AttributeQuery> using browser plug-in. User intent is implied
- User can also sign a <AuthzDecisionQuery>

enspier TECHNOLOGIES

Dynamic Attribute Exchange Profile



Authentication using X.509 certificate

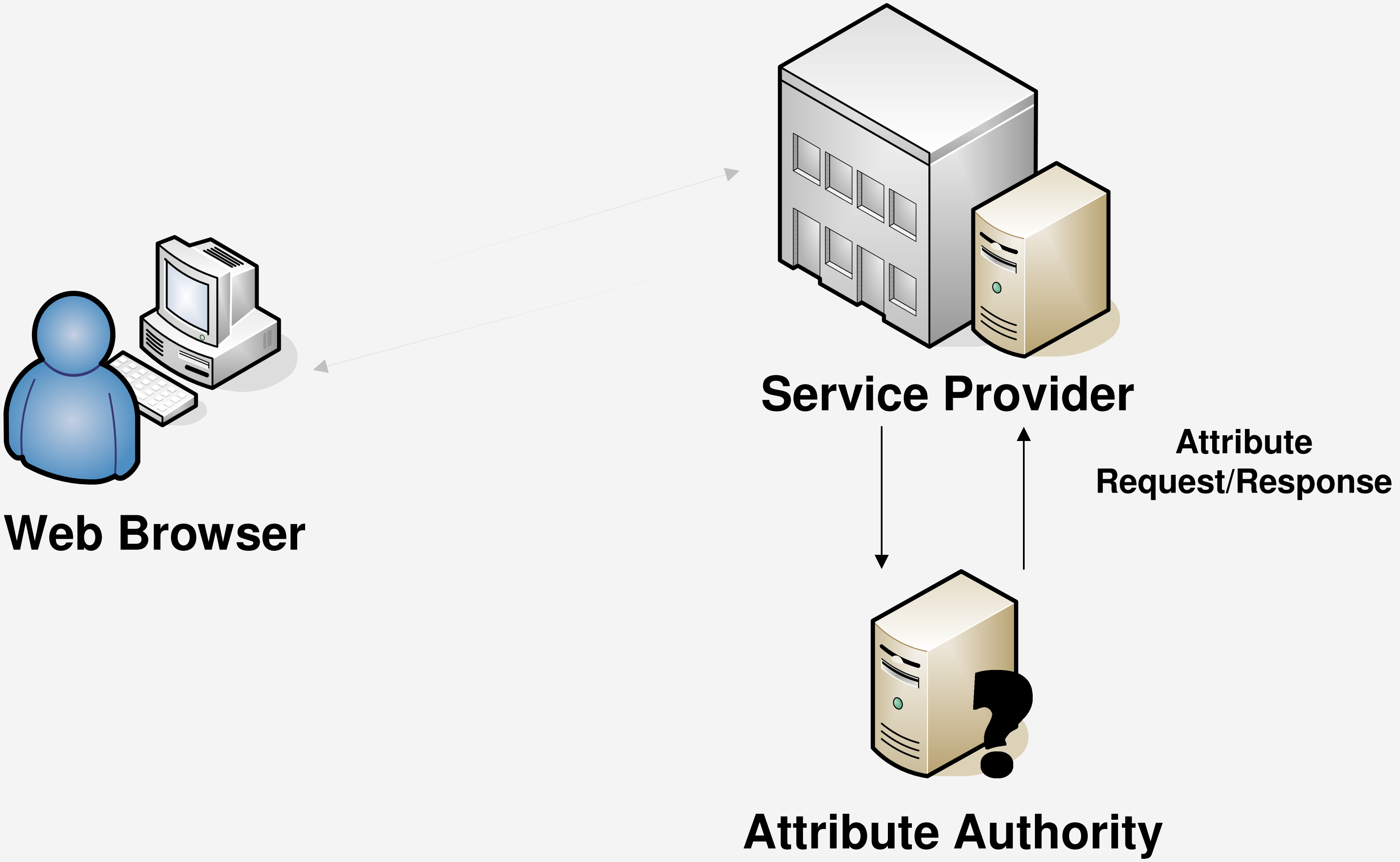
Service Provider

Web Browser

Attribute Authority

enspier TECHNOLOGIES

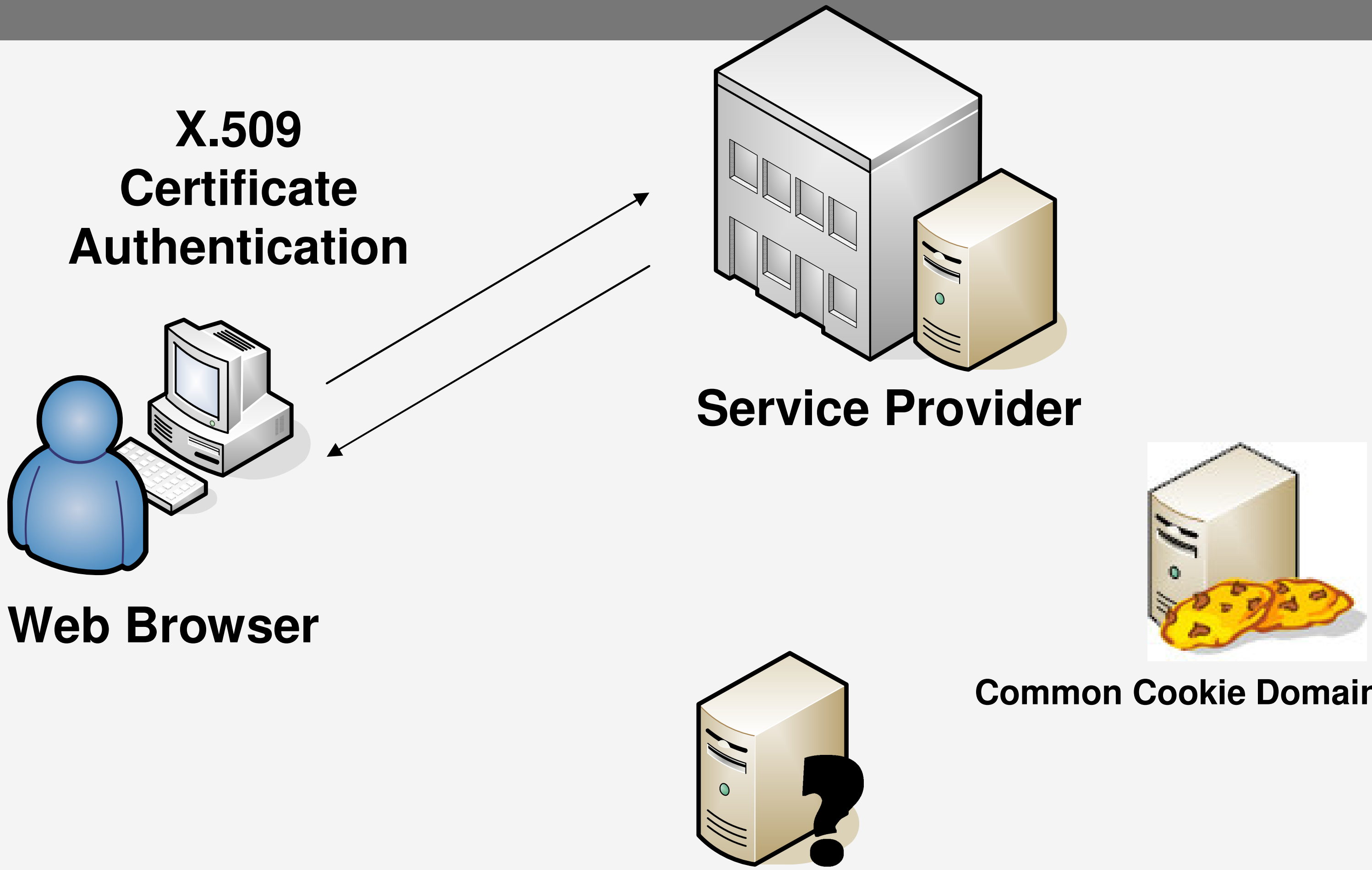
Dynamic Attribute Exchange Profile



Dynamic Attribute Exchange Profile

- End user certificates would not have to be modified with a static extension.
- Third party client side code is not necessary to sign an <AttributeQuery>
- Attribute authority has to be discovered

Dynamic Exchange Profile -- IdP Discovery Profile



X.509 Certificate Authentication

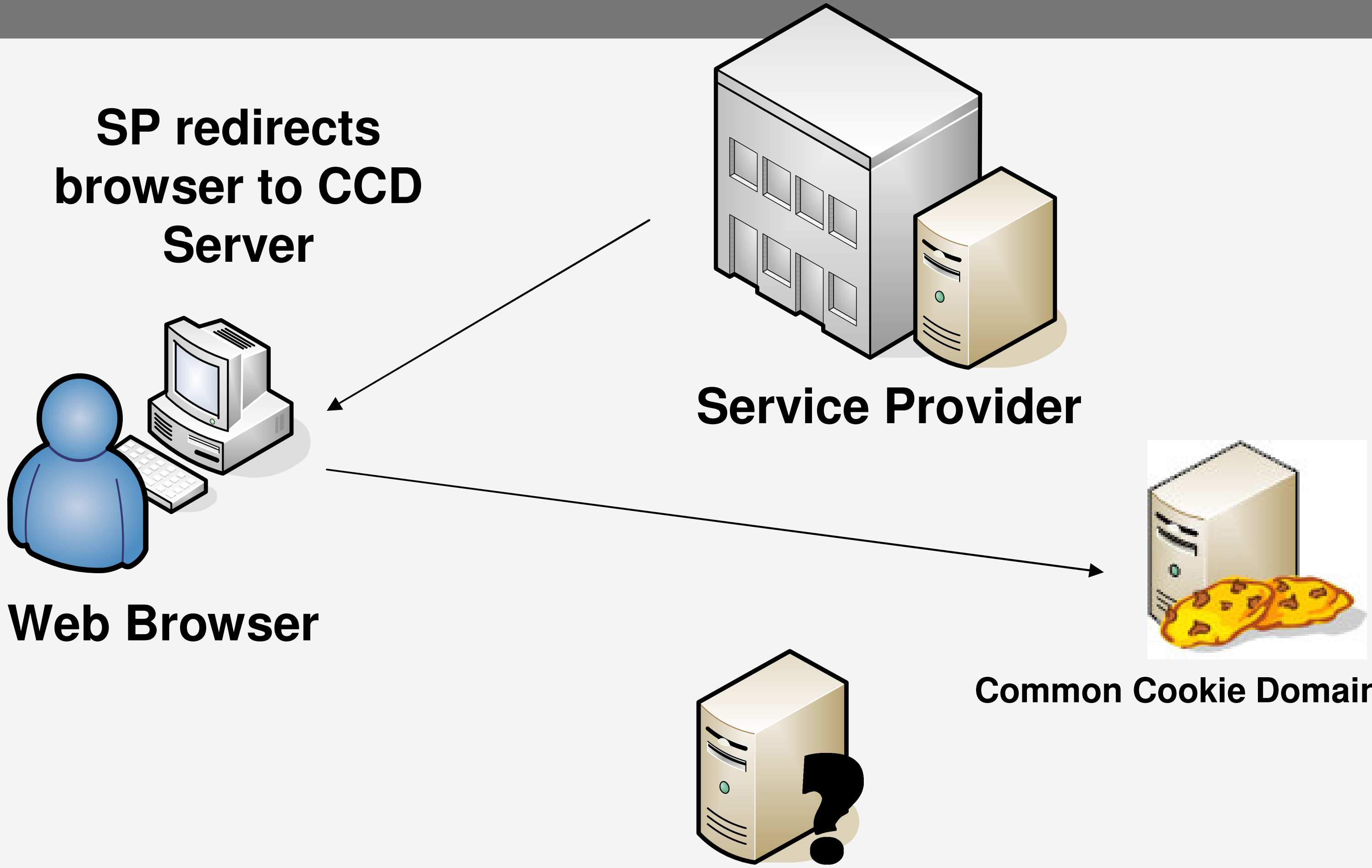
Service Provider

Web Browser

Common Cookie Domain Server

Attribute Authority

Dynamic Attribute Exchange Profile -- IdP Discovery Profile



SP redirects browser to CCD Server

Service Provider

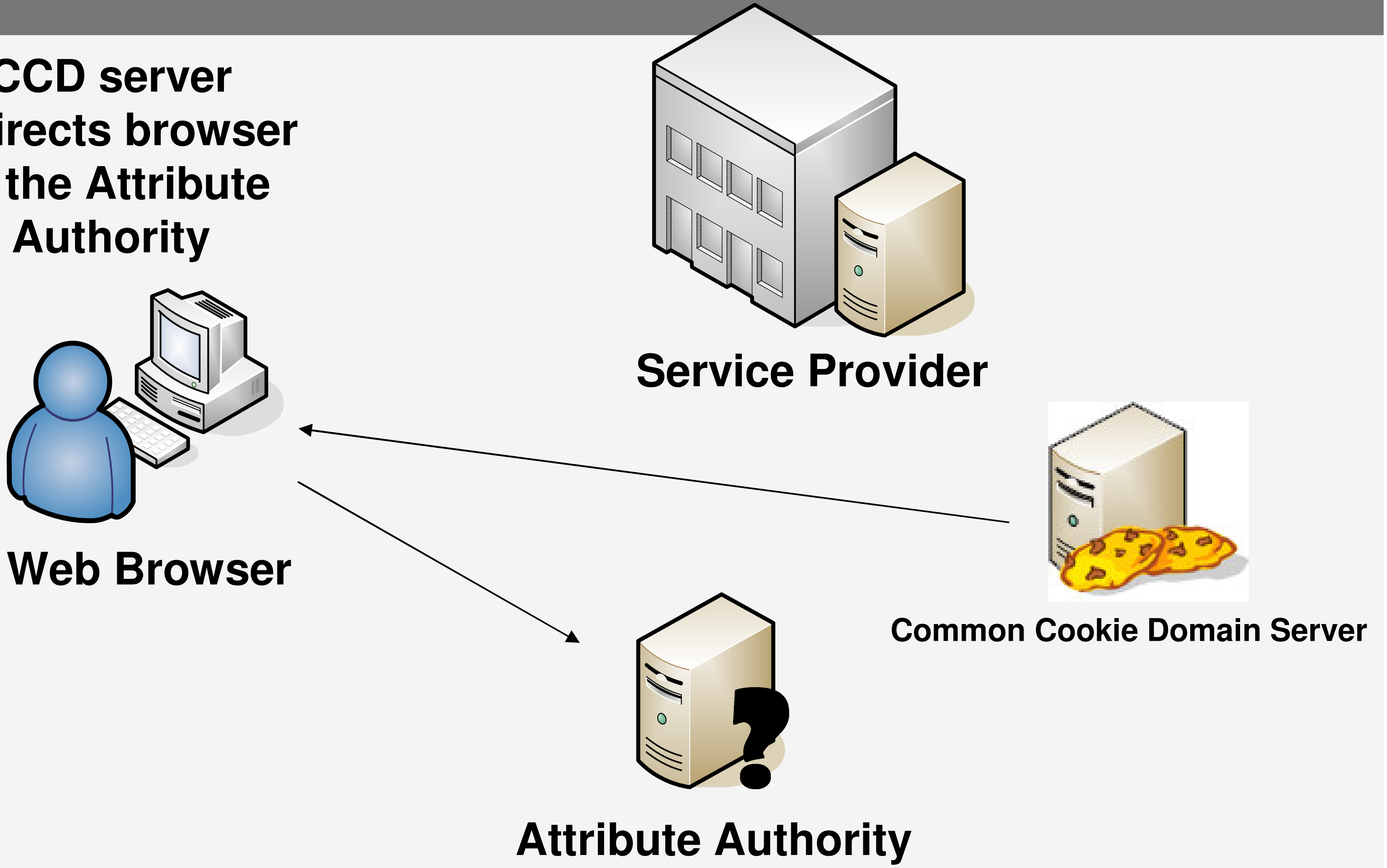
Web Browser

Common Cookie Domain Server

Attribute Authority

Dynamic Attribute Exchange Profile -- IdP Discovery Profile

CCD server redirects browser to the Attribute Authority



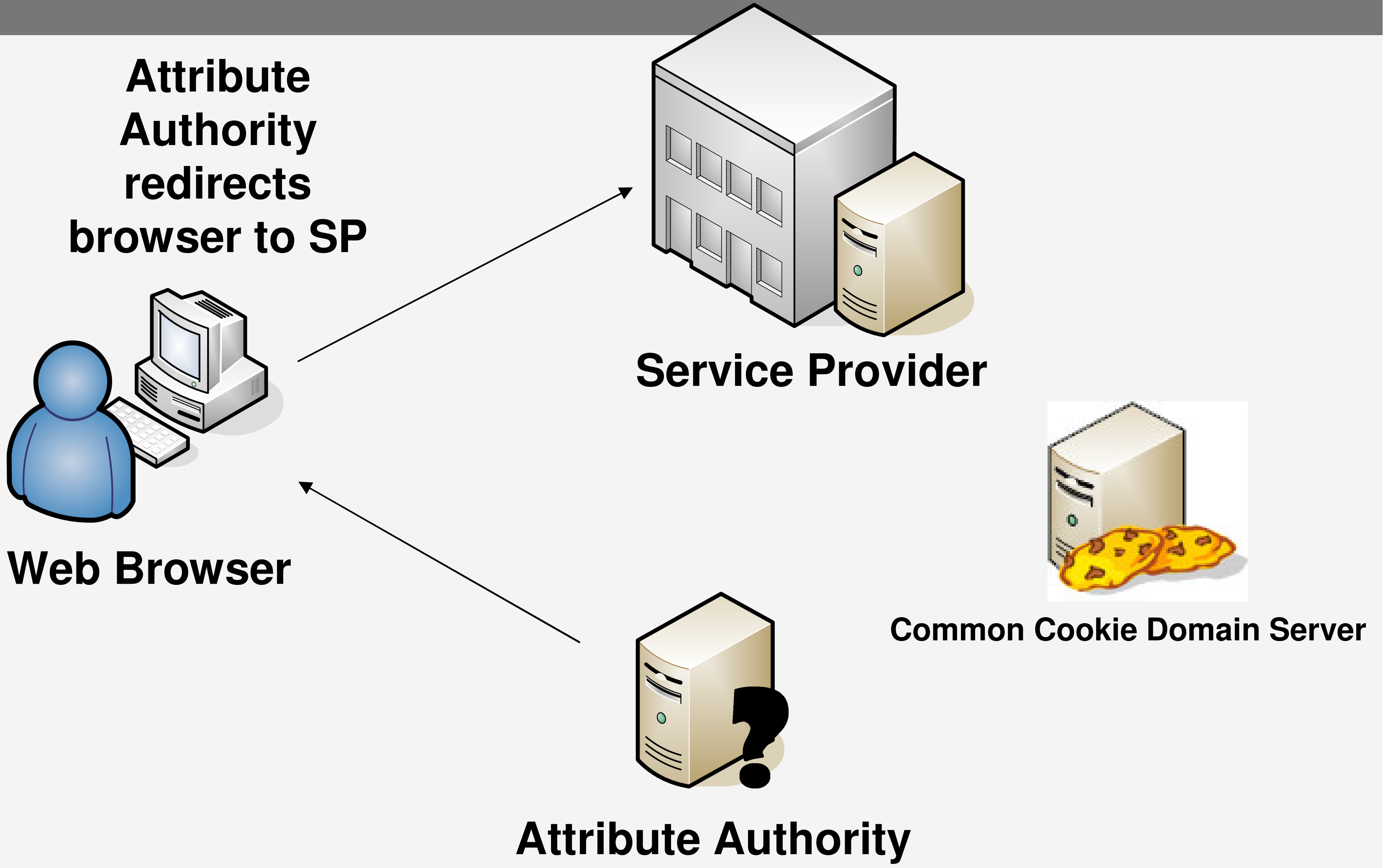
Service Provider

Web Browser

Common Cookie Domain Server

Attribute Authority

Dynamic Attribute Exchange Profile -- IdP Discovery Profile



Attribute Authority redirects browser to SP

Service Provider

Web Browser

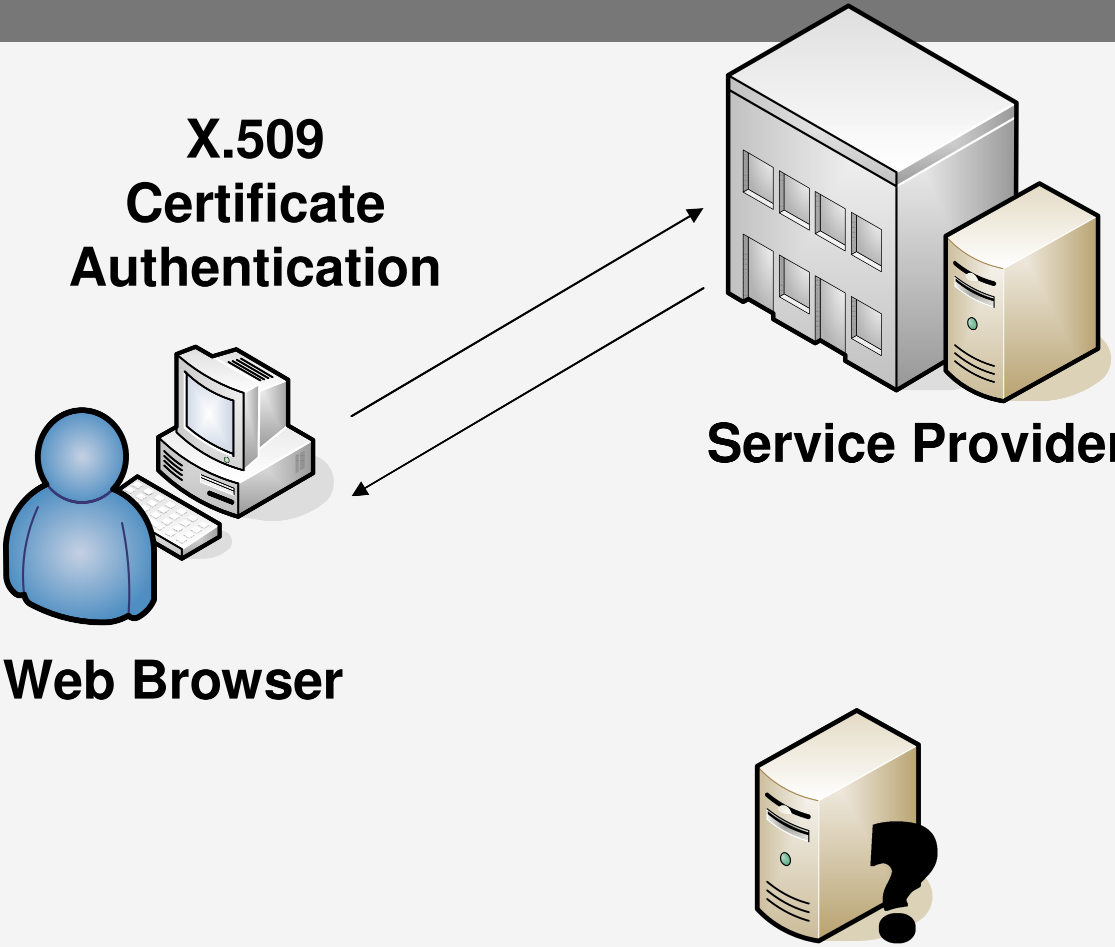
Common Cookie Domain Server

Attribute Authority

Dynamic Attribute Exchange Profile

- Service provider makes educated guess of the appropriate Attribute Authority
  - Issuer name mapping

Dynamic Attribute Exchange Profile – Educated Guess



X.509 Certificate Authentication

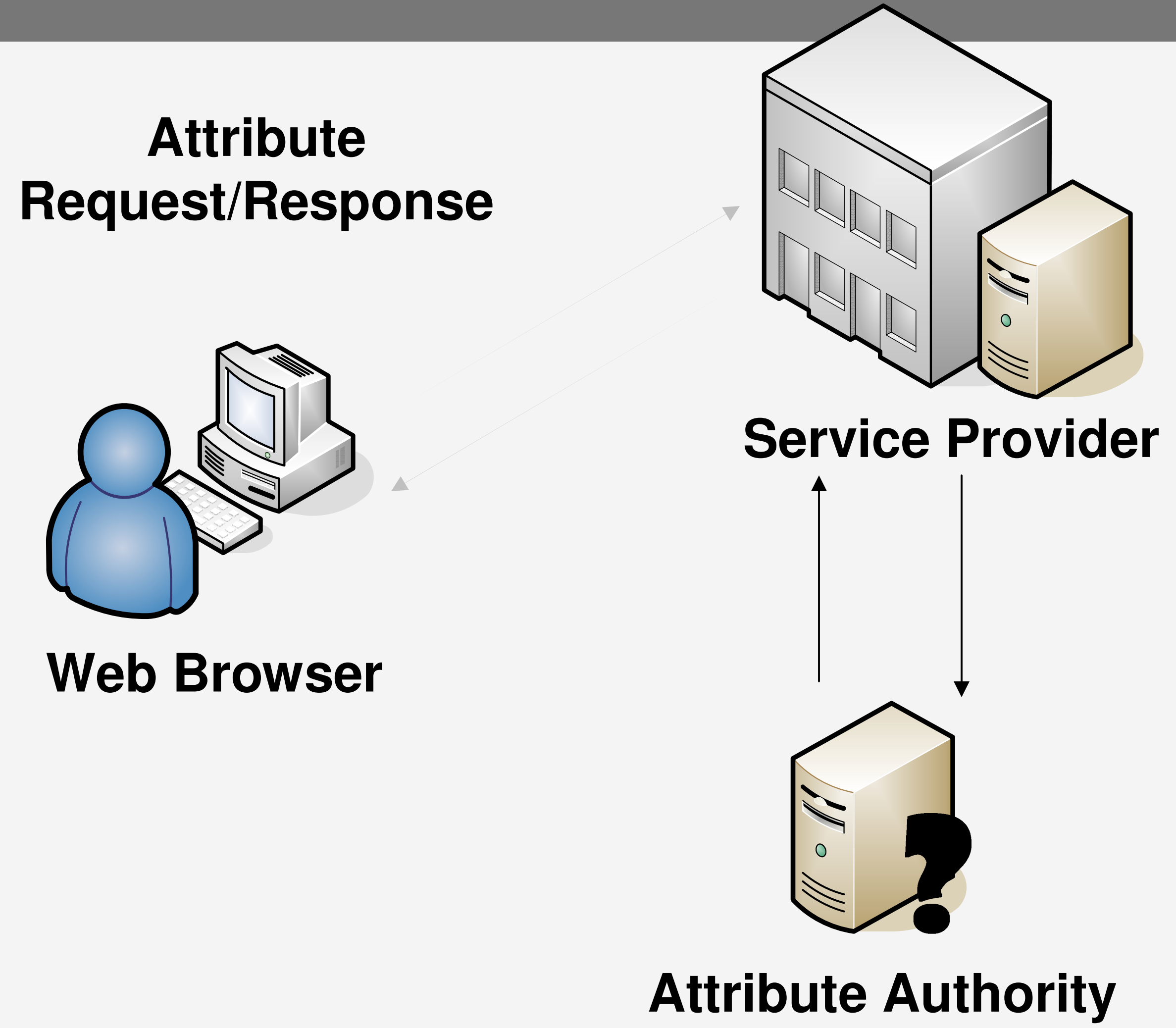
Web Browser

Service Provider

Attribute Authority

enspier TECHNOLOGIES

Dynamic Attribute Exchange Profile – Educated Guess



Agenda

- U.S. Federal E-Authentication Background
- Current State of PKI in E-Authentication
- Future of PKI in E-Authentication
- **Conclusion**

Conclusion

- Current PKI issues can be overcome with SAML 2.0
  - SAML 2.0 provides other benefits
- X.509 credential based SPs can use SAML infrastructure