SAML

Muhammad **Rizwan** Asghar

The University of Auckland

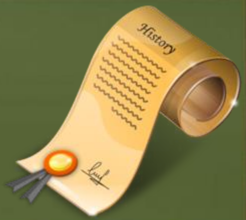
October 8, 2015

For template of slides,
thanks to kingsoftstore.com

Overview

- Security Assertion Markup Language
- Data format for exchanging
  - Authentication data
  - Authorisation data
- XML-based
- Open standard
- A product of OASIS

History



- Developed in January 2001
- SAML 1.0 was adopted as an OASIS standard in November 2002
- SAML 1.1 ratified in September 2003
- SAML 2.0 became an OASIS standard in March 2005

Why SAML

- No standard and interoperable solution for exchanging authentication and authorisation information

Basic Purpose

- Cross-Domain Single Sign-On (SSO) or CDSSO in short
- Identity federation

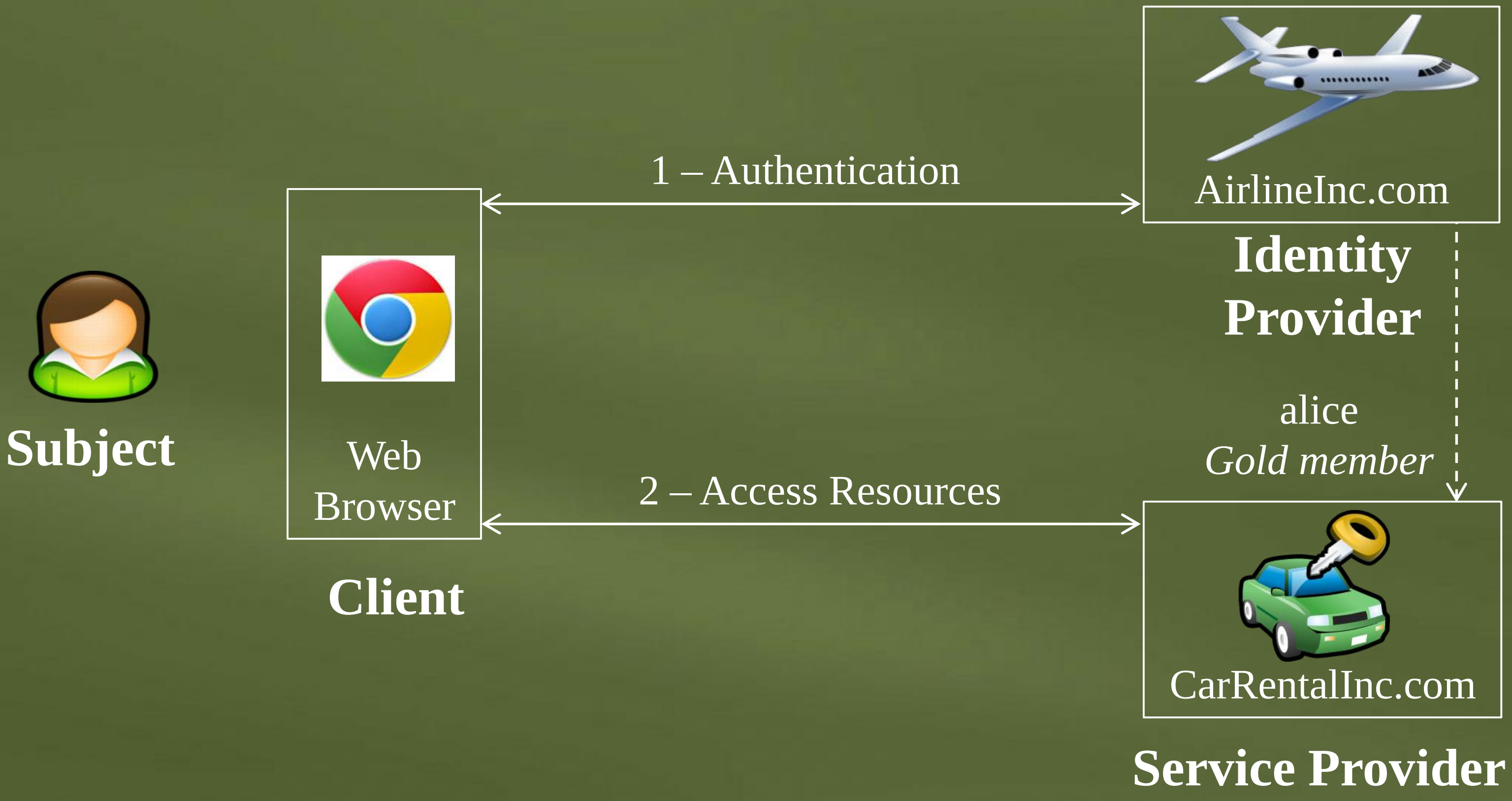
Core Components

- Identity Provider (IdP)
  - Authenticates the user
  - Provides authorisation information
- Service Provider (SP)
  - A server that hosts protected resources
  - It relies on information provided by the IdP
  - Local access policies to regulate access to protected resoruces

Example

- Consider Alice visits an airline website for making her trip
- For booking her flight, she provides her credentials to airline website
- After booking, she found a link to car rental (say from airline website)
- She visits car rental website

SAML Flow


1 – Authentication
AirlineInc.com
Identity Provider
alice
Gold member
Subject
Web Browser
Client
2 – Access Resources
CarRentalInc.com
Service Provider

Example Cont.

- Alice rents a car without signing in again
- CarRentalInc.com trusts AirlineInc.com for authentication

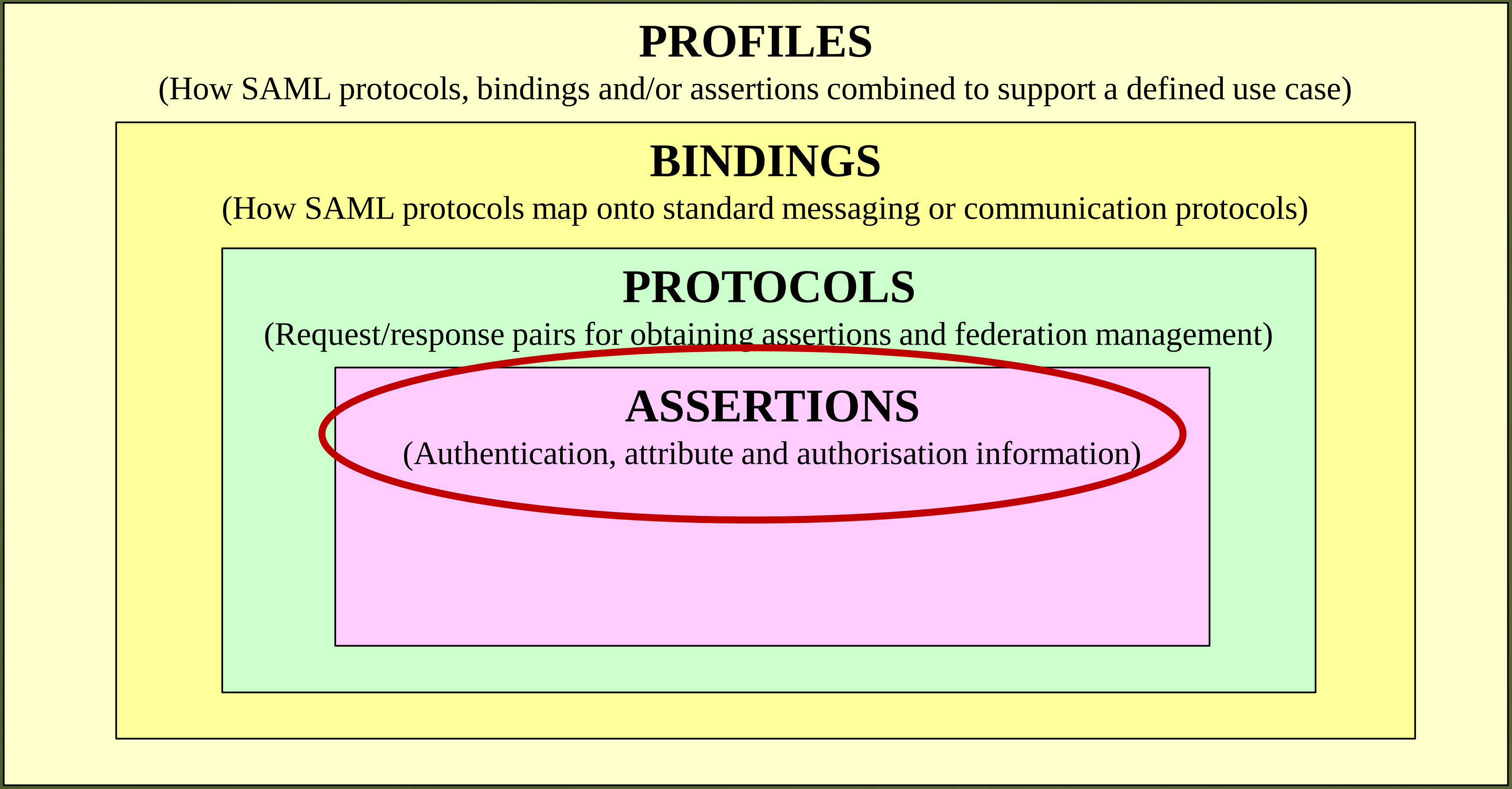
What does SAML Provide? ✓

- Cross-Domain SSO
  - A standard vendor-independent protocol for transferring information across domains
  - It does not rely on cookies
- Federated identity
  - Sharing information about user identities across organisations

SAML Flow Types

- IdP-initiated (push)
  - IdP authenticates first
  - Our example follows the IdP-initiated flow
- SP-initiated (pull)
  - An SP requests the IdP to authenticate the Subject

SAML Components



PROFILES

(How SAML protocols, bindings and/or assertions combined to support a defined use case)

BINDINGS

(How SAML protocols map onto standard messaging or communication protocols)

PROTOCOLS

(Request/response pairs for obtaining assertions and federation management)

ASSERTIONS

(Authentication, attribute and authorisation information)

Assertions

- Assertion is the unit of information in SAML
- To assert characteristics and attributes of a Subject
  - ‘Alice’ is a ‘Gold member’
  - Her email is ‘alice@example.com’
  - She is a member of the ‘Engineering’ group

Assertion Types

- Authentication statement
- Attribute statement
- Authorisation decision statement

Authentication Statement

- Issued by a party that authenticates users
- It describes
  - Who issued the assertion
  - The authenticated Subject
  - Validity period
  - Other authentication-related information

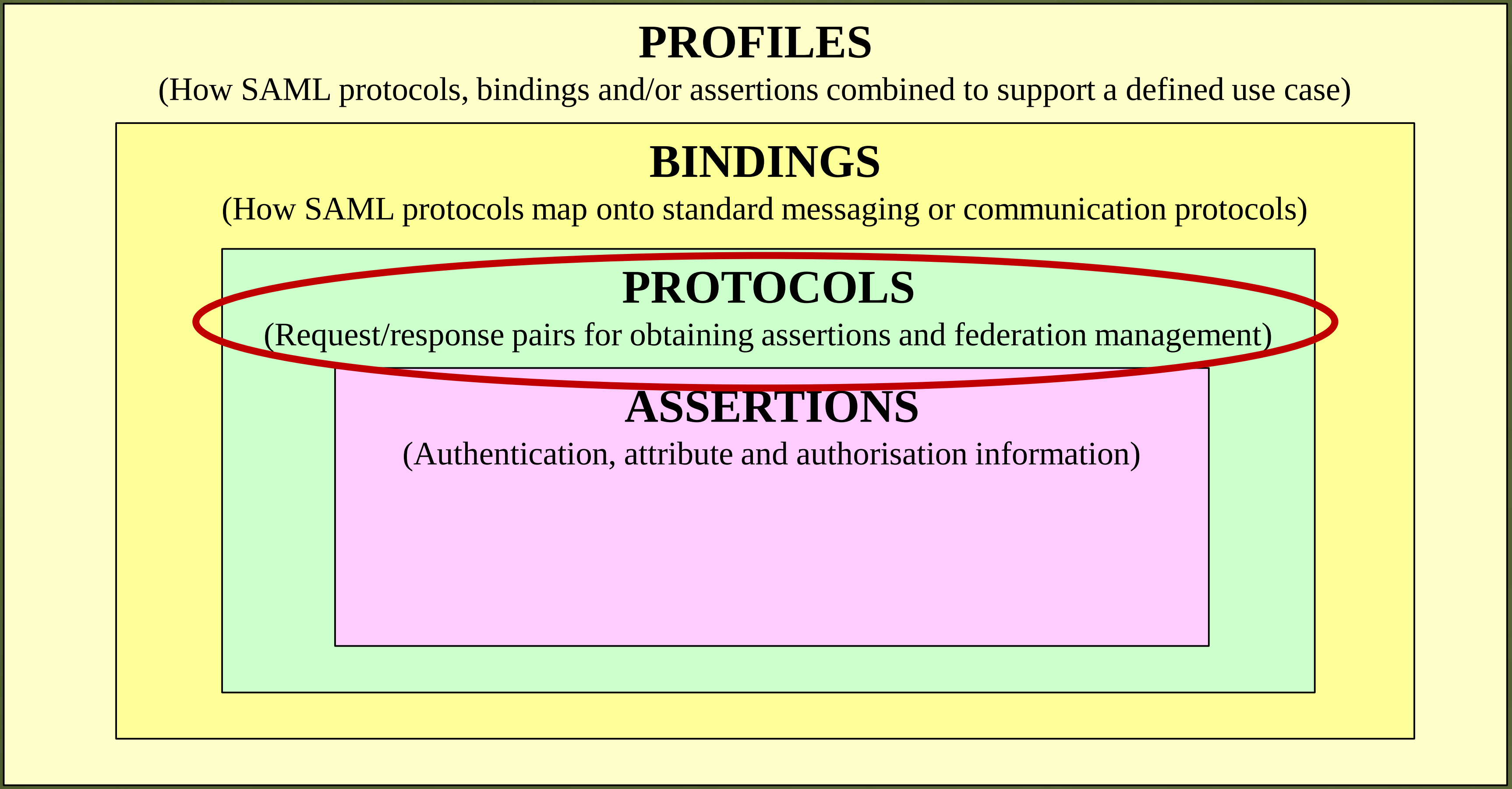
Attribute Statement

- It defines specific details about the Subject
- Examples
  - ‘Alice’ has ‘Gold member’ status

Authorisation Decision

- It defines something the Subject is entitled to do
- Examples
  - ‘Alice’ is permitted to buy a specific item

SAML Components



PROFILES

(How SAML protocols, bindings and/or assertions combined to support a defined use case)

BINDINGS

(How SAML protocols map onto standard messaging or communication protocols)

PROTOCOLS

(Request/response pairs for obtaining assertions and federation management)

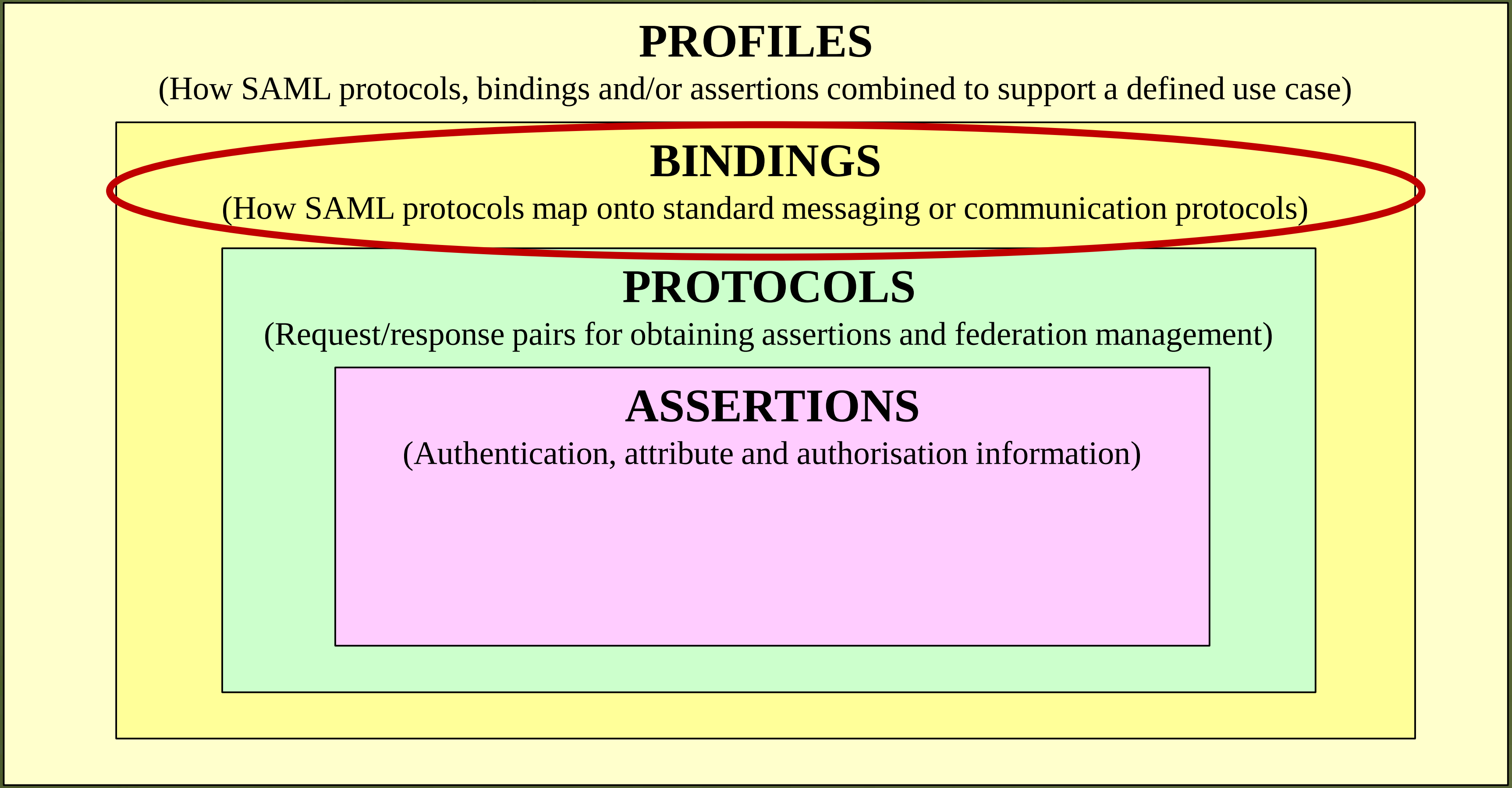
ASSERTIONS

(Authentication, attribute and authorisation information)

Protocols

- Assertion query and request
  - For obtaining SAML assertions
- Authentication request
- Artifact resolution
  - A mechanism by which protocol messages may be passed by references
- Single logout
- …

SAML Components



PROFILES

(How SAML protocols, bindings and/or assertions combined to support a defined use case)

BINDINGS

(How SAML protocols map onto standard messaging or communication protocols)

PROTOCOLS

(Request/response pairs for obtaining assertions and federation management)

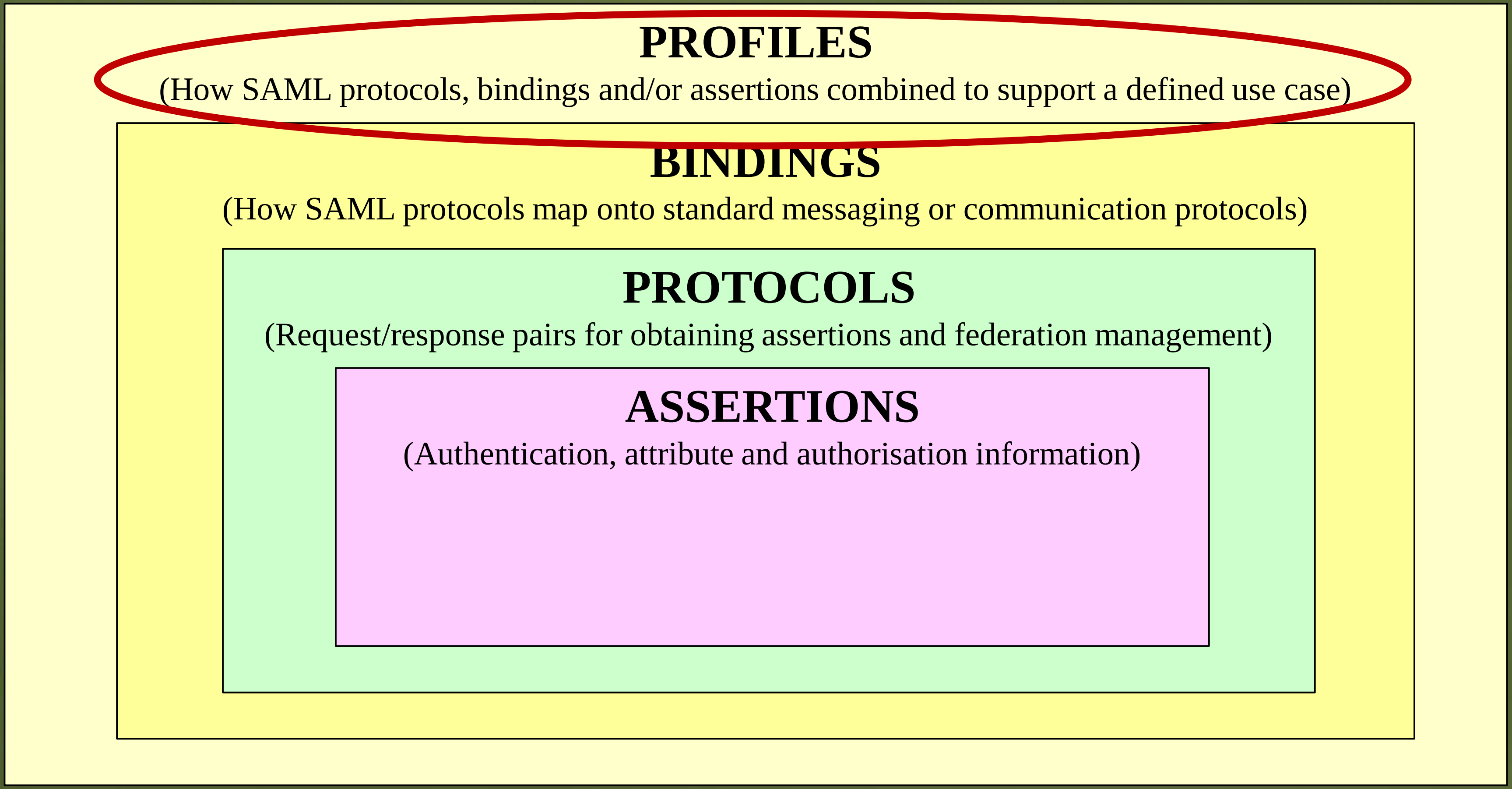
ASSERTIONS

(Authentication, attribute and authorisation information)

Bindings

- SAML URI
- SAML SOAP
- Reverse SOAP (PAOS)
- HTTP redirect
- HTTP POST
- HTTP artifact

SAML Components



PROFILES

(How SAML protocols, bindings and/or assertions combined to support a defined use case)

BINDINGS

(How SAML protocols map onto standard messaging or communication protocols)

PROTOCOLS

(Request/response pairs for obtaining assertions and federation management)

ASSERTIONS

(Authentication, attribute and authorisation information)

Profiles

- Web browser SSO
- Enhanced Client and Proxy (ECP)
- Identity provider discovery
- Artifact resolution
- Assertion query/request
- …

SAML vs SSO

- SSO uses browser cookies to maintain state so that re-authentication is not required
- But browser cookies are not transferred across domains
- Using assertions, SAML offers SSO across domains

Security Requirements

- Mutual authentication
- Integrity
  - Message insertion
  - Message modification
- Confidentiality
- Man-in-the-middle attack
- Replay attack

Security Considerations

- The SAML specifications recommend a variety of mechanisms
  - SSL 3.0 or TLS 1.0
  - XML signature and encryption

Summary

- An open standard for exchange of authentication and authorisation information
- It enables CDSSO and federated identity
- Shibboleth is built on top of SAML

Q&A

References

- SAML V2.0 Technical Overview, https://www.oasis-open.org/committees/download.php/14361/sstc-saml-tech-overview-2.0-draft-08.pdf
- Web Services Security: SAML Token Profile 1.1, https://www.oasis-open.org/committees/download.php/16768/wss-v1.1-spec-os-SAMLTokenProfile.pdf