Introduction & Motivation

• A study by Oracle predicted $85 billions worth of market share for context-aware services by 2015 [1].
• However, there are many unresolved security and privacy issues that need to be addressed to harness the full potential of such context-aware services.
• Most importantly, there is a lack of a framework based on standardised techniques satisfying different security and privacy requirements.
• CAFS (Context-Aware Federated Services) Framework has been developed using standardised technologies such as Security Assertion Markup Language (SAML) and eXtensible Access Control Markup Language (XACML).
• It allows users to have full control over contextual data & to access services securely and seamlessly using Single Sign On (SSO).

State of the Art

• Context represents dynamic attributes: a user’s partial identity, the physical location, the time and date of the service request and the application domain of the Identity Provider (IdP) or the Service Provider (SP).
• In the current setting, users usually share contexts anonymously.
• This preserves privacy, but, personalised services requiring other contexts are difficult to provide.
• The experience can be hugely uplifted by utilising a Portable Personal Identity Provider (PP-IdP) [2] to create federations, to leverage the Single Sign On (SSO) feature and provide context-aware federated services.

Portable Personal IdP (PP-IdP)

• The PP-IdP is a special type of IdP that is hosted in a mobile device owned and/or used by the user and is under the full control of the user and has two components: Personal Attribute Store (PAS) and IdP.
• The PAS Control Panel can be used to manually add/update user attributes and then store them securely in a database.
• The PAS can also use phone’s sensors to read contextual data and store them as user attributes into the database.
• The PAS and the IdP have been developed for Android as Apps. The servlet container has been deployed using the embedded Jetty Web Server.

Use-Case: Protocol Flow-1

• Based on CAFS Type 1 where location data is provided by the PP-IdP.

Use-Case: Protocol Flow-2

• Here, location must be read from the QR Code and provided by the PP-IdP.

Use-Case: Settings

• Each SP has a few web pages protected using the PEP developed in PHP.
• The Table specifies the list of attributes required for each page in the respective SP.
• val - geographic values: (55.865318, -4.267437), (55.865185, -4.2660857), (55.864722, -4.266203), (55.864806, -4.268220).
• The gte means “greater than or equal”, the equals signifies a match, the within signifies location are within the specified value & between signifies the duration.
• Verifiable location data are generated by QR Codes.

Advantages

• CAFS is the first framework to demonstrate how contexts can be used to provide federated services using SAML and XACML.
• The user utilises SSO feature of the IdP reducing logins for separate services.
• We also show how the user can be located precisely and securely inside a building using external sensors (camera) of smartphones.

Future Work

• To choose different attributes without initiating a new flow.
• To aggregate attributes from other IdPs.

References