The Vision

Resilient Access virtualizes real-world relationships and conditions of trust, resolve identities in the network, and enforce each party's policies. This enables disparate organizations and users to share sensitive information and applications while maintaining control and privacy. Enterprises, government agencies, and online platforms leverage Resilient Access to collaborate and share information with their ecosystems of partners and customers.

Resilient Access Policy Evaluation

We have taken the first steps in realizing that vision by building a dynamic distributed policy evaluation engine. The core tenets of this policy evaluation engine is there is no one party that acts as the gate keeper making the final policy decision like in the federated model. Policy evaluation is "syndicated" across the different parties that are involved in making the policy decisions.

Syndication and dynamic Policy evaluation

Resilient Access policies are logical expressions that reference one or more Authorities. An authority performs an evaluation function that in the basic case generates an GRANT or DENY decision. A policy evaluates to a GRANT if the Authorities that are part of the policy expression evaluates to grant. For example the Policy:
EmailAuthentication AND PhoneAuthentication
will evaluate to a GRANT if both the EmailAuthentication and PhoneAuthentication authorities evaluate to a GRANT.
An Authority can also return a third state and that is another Policy. This is the mechanism through which dynamic policy evaluation takes place that can address syndication and cross-organizational policy evaluation use cases. An use case that illustrates this is of a doctor attempting to attain the medical record for a patient. Lets assume there is a syndicate consisting of medical institutions, pharmacies and insurance companies. Doctors are associated with medical institutions, patients are associated with a medical institution and an insurance company. The syndicate uses the Resilient Access for managing the policies that would grant access to sensitive medical records. The syndicate operator may create a high level policy such as IsDoctor(DoctorID) AND IsPatient(PatientID) to facilitate the access of a patient's medical record by a doctor. Lets assume the DoctorID identifies the medical institution the doctor is associated with and the PatientID identifies the insurance company the patient is a member of. The syndicate operator will then forward the policy evaluation to the medical institution for the doctor and the insurance company for the patient. Each medical institution and insurance company that is part of the syndicate can define their own policy for validating that the doctor or patient is a member of their organization.

Privacy enhancing features

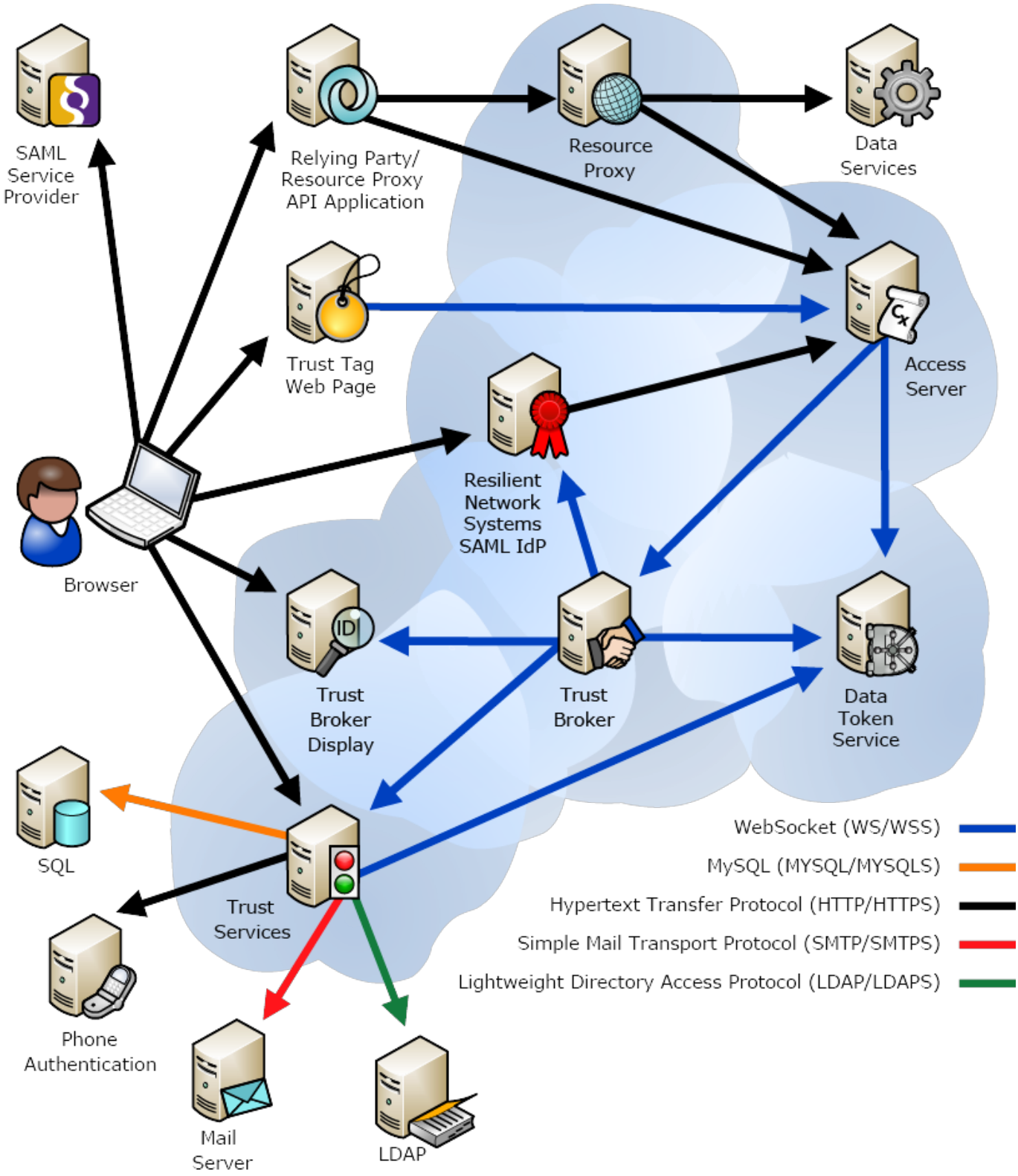
Policy evaluation in Resilient Access contains various privacy enhancing features. Policies can be crafted such that sensitive information does not flow through the network. The only party that would request for a sensitive data item would be the authority that requires the particular data item in order to perform its policy evaluation tasks. An example of this is an LDAP Authentication Authority that need an UserID and a Password to perform its evaluation. The sensitive data item in this case is the password. The policy

can be created such that this data item is not requested from the user when the policy evaluation commences. Only when the evaluation sequences arrives at the LDAP Authentication Authority, it will ask for the password through a Display Request that is posted to the user.

The other mechanism for privacy enhancement is through data obfuscation, or Zero Knowledge. In this case if sensitive personal identity information (PII) needs to flow through the network as part of a policy evaluation, policy can be crafted such that the PII data item is converted into an opaque token with the rules that the only party that can de-tokenize it is the Authority that is specified when the token is created. An example of this is say one Authority receives an email address, performs a database lookup and retrieves a SSN that need to be sent to another authority that can perform an evaluation based on the SSN. Instead of passing the sensitive info through Resilient Access un-encrypted the first authority can use a Data Token Service to obfuscate the SSN and identify the second authority as the one that can get the un-obfuscated value.

Resilient Access Components

The following diagram shows the components of Resilient Access and the relationship among them.



The Policy Workflow Engine

The Policy Workflow Engine is the orchestrator of the policy evaluation. It receives the policy expression from the Policy/Authority Store and routes the evaluation to the authorities. It uses the Trust Broker

Display to post the display request screens for additional credentials required by the policy. At the end of the evaluation it returns the result to the Access Server

Policy/Authority Store

The policies are configured in the Access Server. The Policy/Authority Store provides a Relying Party API for external services to connect to Resilient Access. Resilient provides several implementations of the Relying Party including Trust Tag, Data Proxy and SAML Identity Provider.

Authority Credentials

Authority Credentials act as the agent of the Policy Workflow Engine that interacts with the Browser. It manages the Trust Session that maintains the information of granted policies. Authority Credentials also redirects the browser to the Authorities Display Request screen as well as back to the Access Server at the end of policy evaluation.

Data Token Service

The Data Token Service provides an API for obfuscating data items into tokens. At the time the token is created the address of the service that can de-tokenize the data is also provided to the API. Only the service that has the permission to de-tokenize can retrieve the data value.

Authorities

Authorities perform an evaluation function and returns GRANT or DENY or another policy. If an authorities requires additional credentials then it sends a DISPLAY_REQUEST response to the Trust Broker for it to initiate a Display Request sequence through the Trust Broker. Resilient provides various types of authorities. These fall under the following broad categories:

- LDAP/AD Based Authorities - connects to an LDAP/AD and verifies identify such as password match (e.g. Password Authentication) or compares attributes retrieved from the LDAP/AD with expected values (e.g. Role Authorization)
- Database Authorities - connects to a Database and executes the configured SQL query for identity verification (e.g. Database Authentication) or compares data retrieved from the Database with expected values (e.g. Data lookups)
- User Created Authorities - these authorities integrate to services provided by third party identity or authentication service vendors. This category can also be used to build custom authorities that perform identity and authentication functions specific to an organization
- Policy Authorities - facilitates dynamic policy evaluation by retrieving attributes from LDAP/AD, Database or custom APIs and substituting them into the parameters of another policy. E.g. retrieve a phone number from an LDAP/AD and insert it into a Phone Authentication output policy