Goal: A scalable means of access control for widely distributed resources, supporting: ① bilateral trust establishment, ② run-time access control policy discovery, ③ client and resource privacy, and ④ legacy and trust-aware resources.

Approach: A Credential Translation Service that uses automated trust negotiation to map sets of attestations issued by well-known external entities into locally-meaningful access credentials.

Design: The Credential Translation Service utilizes the TrustBuilder framework for automated trust negotiation to conduct trust negotiation sessions within the TLS protocol.

Usage Scenarios:

Legacy Scenario: Loose binding of resource and Credential Translation Service

1. Alice contacts cts.stocks.com to request credentials to access purchase.stocks.com. After trust negotiation, she receives a SAML assertion that states she is currently authorized in the stocks.com security domain.
2. Alice sends purchase.stocks.com the SAML assertion to gain access to the service.

Trust-Aware Scenario: Tight binding of resource and Credential Translation Service

1. Alice makes initial contact with gridftp.bigstorage.com, which refers her to cts.bigstorage.com for authorization.
2. After a trust negotiation with cts.bigstorage.com, Alice receives the X.509 proxy certificate needed to log into gridftp.bigstorage.com.
3. Alice changes directories; gridftp.bigstorage.com informs her that she must present new access credentials.
4. Alice negotiates with cts.bigstorage.com to obtain the X.509 proxy certificate needed to access the new directory.
5. Alice sends her new X.509 proxy certificate to gridftp.bigstorage.com and is granted access to the desired directory.

The iterative nature of automated trust negotiation allows resource access policies to be discovered incrementally, disclosing more of the relevant policies as the trust between the client and credential translation service grows. The bilateral nature of automated trust negotiation allows Alice to request credentials from the Credential Translation Service before disclosing sensitive information of her own.