Pulse2011

Smarter IAM – QLD DET

The Education Challenge

Mark Johnston
IBM Security Solutions Architect

Introduction

- Mark Johnston
  - Security Solutions Architect, SWG Security Tiger Team
  - Last 2 years in Brisbane working on QLD Government Identity and Access Management programs of work as part of, Security and Privacy Practice, GBS
  - 10 Years in IT, 6 specifically IAM

Agenda

- About QLD Department of Education and Training (DET)
- IAM Challenges in Education
- DET's solution requirements
- Why IBM?
- DET IAM integration overview
- A platform for secure IT growth in DET

About QLD DET

- Smart Classrooms Program
- 700,000 user identities utilising, 300,000 desktops statewide
- 13 AD Forests, over 1300 domain controllers
- 380,000 Password resets in first week of school
- OneSchool application during school reporting averages 16,500 unique sessions, 1.3 million pages a day
- Multiple silo'd application owners and technologies within.

IAM Challenges in Education

- Large scale, high churn in small time periods
- Things can't change…
- Content access and delivery is key - EdTube
- Compliance with regulatory requirements
  - – Identity Protection
  - – Auditing and reporting
- Disparate technology stacks
  - – many vendors many products
- Security vs. Practicality
  - – Password Complexity
  - – Application idle timeouts

DET Solution requirements

- A Single extensible application SSO framework that would replace all others in the environment
- Design, develop and build an RBAC and RBP model for provisioning application access
- Tight coupling with existing .NET and AD Authentication frameworks
- Centralised, audit and reporting solution
- Flexible foundation for IAM

Why IBM?

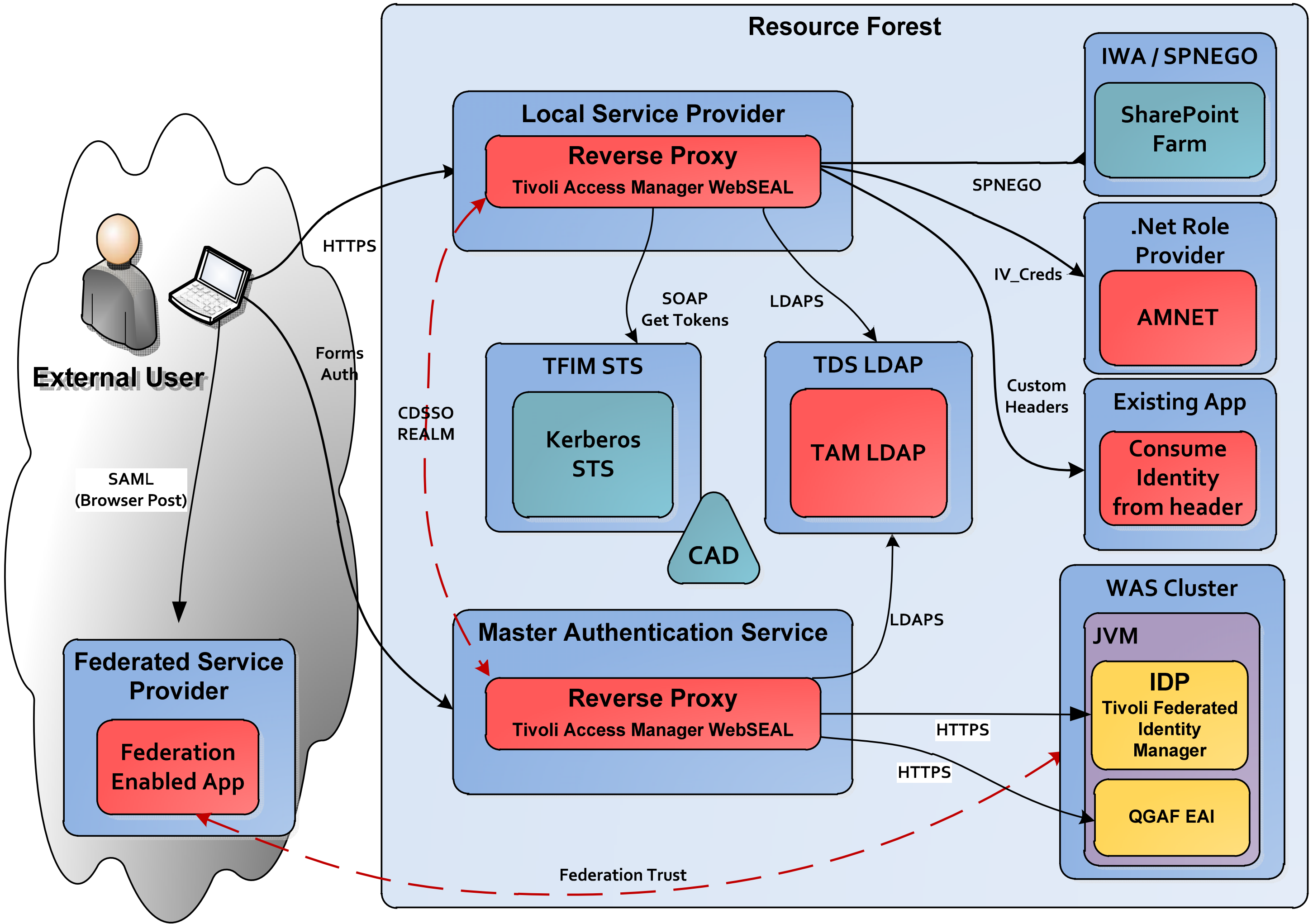
- Demonstrated expertise in delivering complex IAM solutions.
- Maturity of IBM security frameworks and methodologies
- Competence in all areas of the SDLC – design, build, operate.
- Ability to bring together and deliver solutions to meet businesses requirements
- Capability in delivering an integrated solution using Tivoli and Microsoft products

DET’s Primary Applications

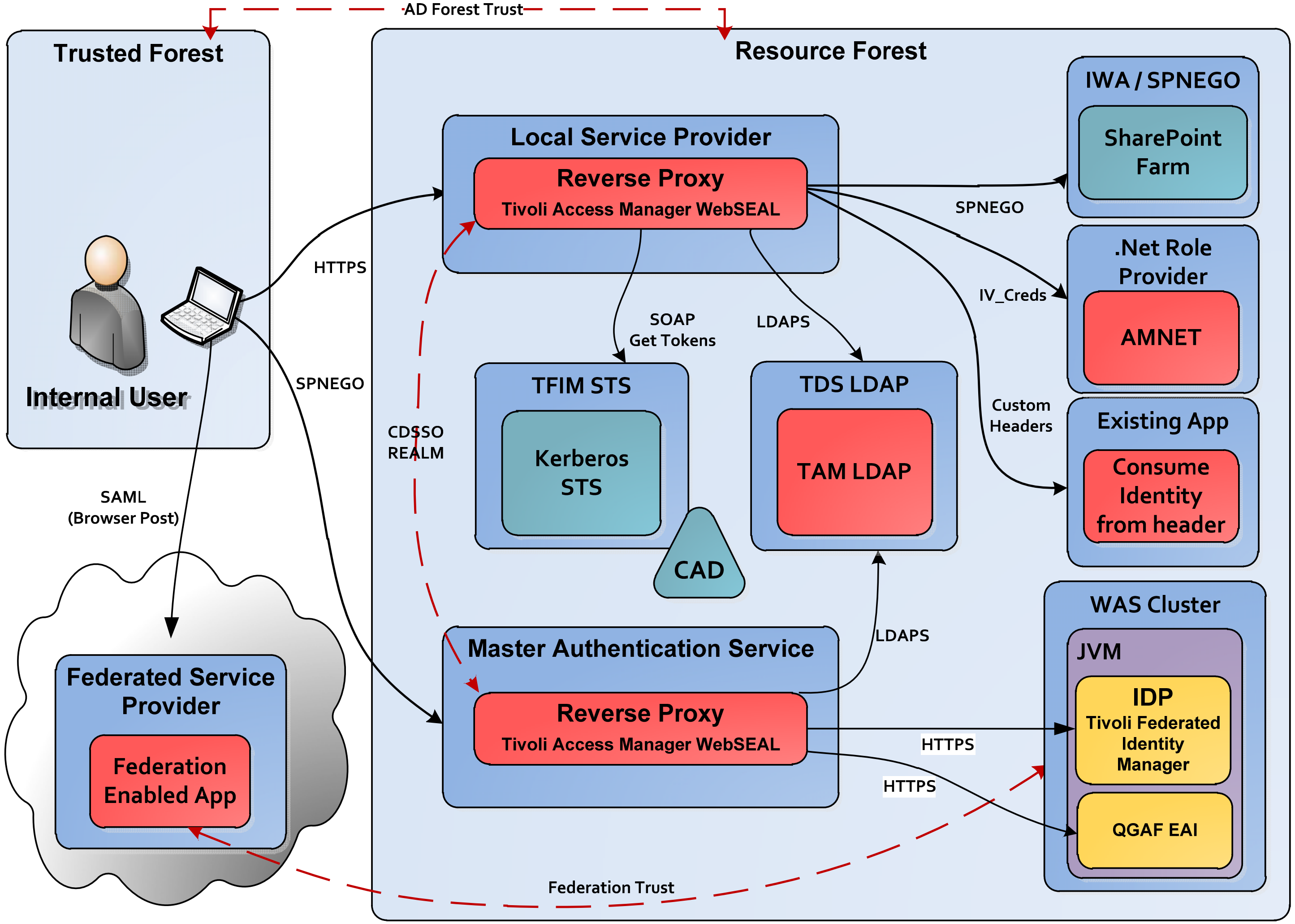
- The Learning Place
  - A suite of applications designed for facilitating learning, course management and creation of generic identities.
- OneSchool
  - QLD DETs custom developed .NET application for school enrolment, scheduling, reporting and finance.
- OnePortal
  - Corporate intranet Sharepoint consisting of Intranet, My Sites and Team sites.
- iRegister
  - Custom developed .NET 3.5 application for Registration and Enrolment of corporate and school staff.

DET – SSO

Access Management - External

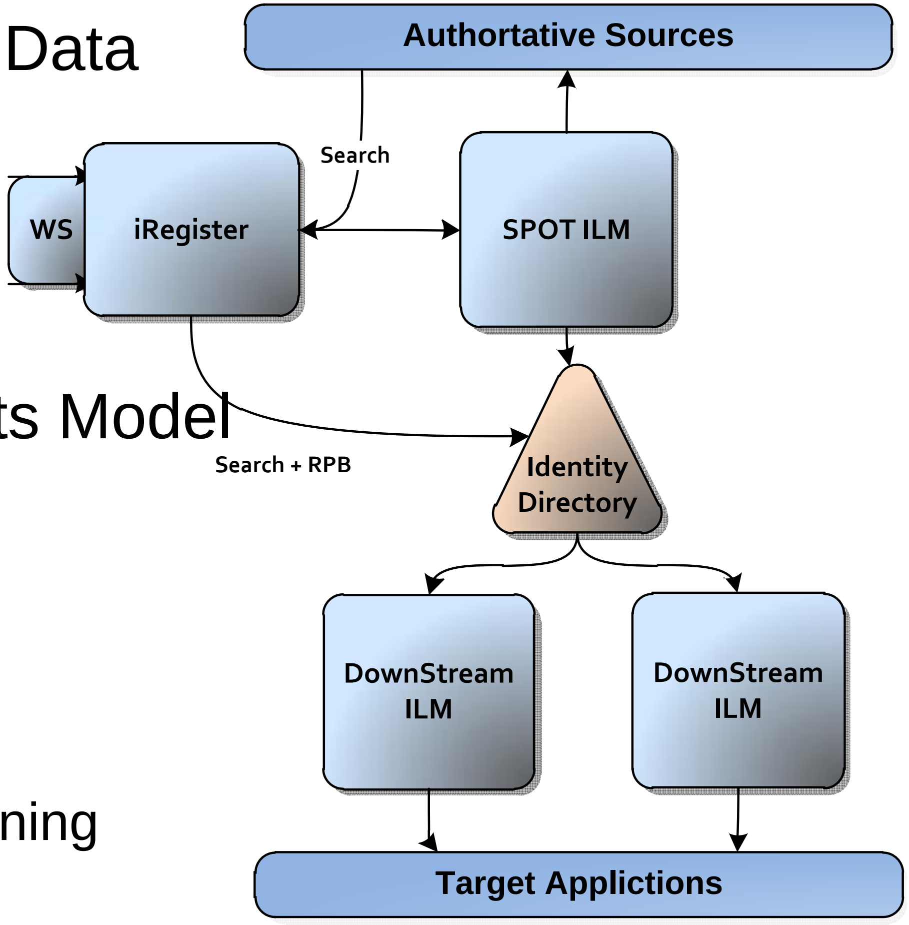


Access Management - Internal



Identity Management and iRegister

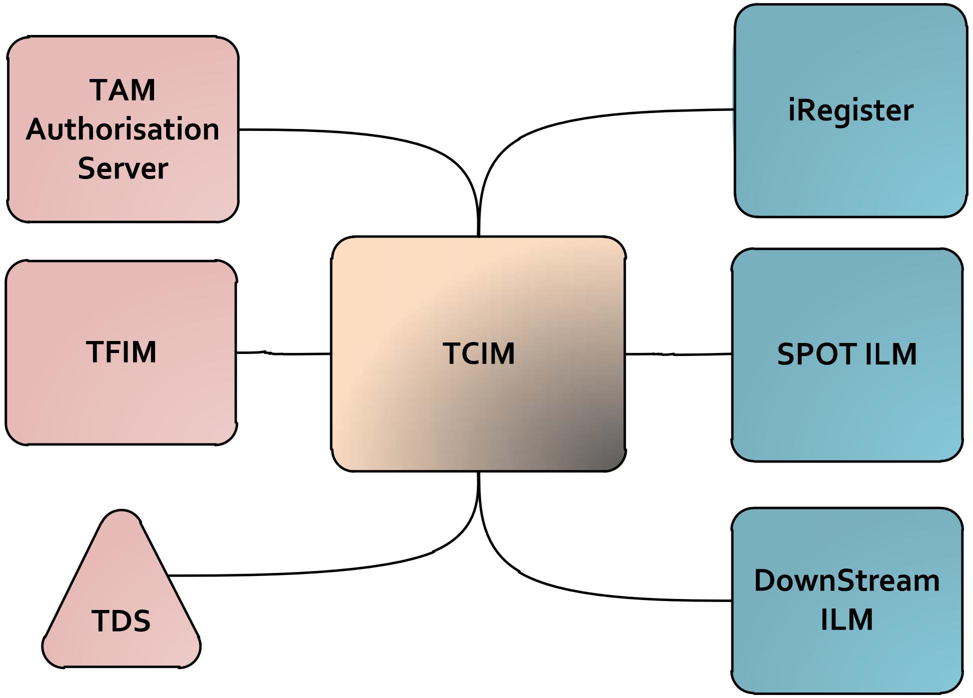
- 13 Authoritative Sources of ID Data
- 17 Target Systems / Apps
- Microsoft ILM 2007



- Custom developed Entitlements Model
- iRegister
  - Custom .NET Web Application
  - Self Registration
  - Request Based Provisioning
  - WebServices search and provisioning
  - My Identity page

Audit and Reporting Overview

- TCIM
- COTS Actuators for TAM / TFIM / TDS
- W7 XML from IDM
- W7 CSV from iRegister

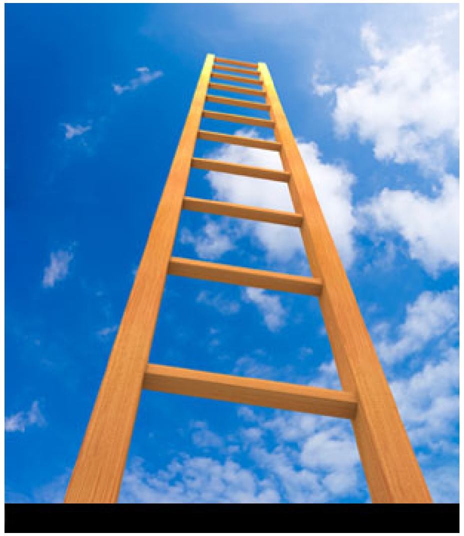


Platform for Secure IT growth in DET

- Secure re-usable authentication and identity services
  - Implemented ability to comply with QGAF without modifying application.
- PKI Infrastructure
  - SSL Key lifecycle management
- Strategic IAM Testing / Integration Platform
  - Mirrored Production environment
- Zoned Network Infrastructure.
  - Layered network tiers for migration from existing environment.

Next steps

- Upgrades in progress
  - ForeFront Identity Manager
  - TSIEM 2.0
- Grow maturity of Enterprise roles framework
- Integration of further applications / services ready for integration with WOG services



"Even if you are on the right track, you'll get run over if you just sit there."

~Will Rogers~

Questions…

Thank You!

Trademarks and disclaimers

The customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.

Information concerning non-IBM products was obtained from a supplier of these products, published announcement material, or other publicly available sources and does not constitute an endorsement of such products by IBM. Sources for non-IBM list pricesand performance numbers are taken from publicly available information, including vendor announcements and vendor worldwide homepages. IBM has not tested these products and cannot confirm the accuracy of performance, capability, or any other claims related to non-IBM products. Questions on the capability of non-IBM products should be addressed to the supplier of those products.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Some information addresses anticipated future capabilities. Such information is not intended as a definitive statement of a commitment to specific levels of performance, function or delivery schedules with respect to any future products. Such commitments are only made in IBM product announcements. The information is presented here to communicate IBM's current investment and development activities as a good faith effort to help with our customers' future planning.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Prices are suggested U.S. list prices and are subject to change without notice. Starting price may not include a hard drive, operating system or other features. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Photographs shown may be engineering prototypes. Changes may be incorporated in production models.